LABOR RELATIONS

UNITED STATES POSTAL SERVICE

RECEIVED
MAR 24 2021

March 23, 2021

RECEIVED
MAR 24 2021

Mr. Brian J. Wagner
President
National Association of Postal
Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Dear Mr. Wagner:

As a matter of general interest, the Postal Service is revising Handbook AS-805, *Information Security*.

The subject revisions establish policy concerning cybersecurity roles and responsibilities, including the protection of sensitive data and separation policies for departing personnel.

We have enclosed two copies of the revised Handbook AS-805, one with and one without changes identified.

Please contact Bruce Nicholson at extension 7773 if you have questions concerning this matter.

Sincerely,

David E. Mills
Manager
Labor Relations Policies and Programs

Enclosures

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4101
WWW.USPS.COM

1 Introduction: Corporate Information Security

1-1 Purpose

The Postal Service™ is committed to creating and maintaining an environment that protects Postal Service information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. Information resources are strategic assets vital to the business performance of the Postal Service. Refer to Exhibit 1-7 for examples of information resources. Information resources are also protected by law and governed by law. Handbook AS-805, *Information Security,* establishes an organization-wide standardized framework of information security policies to ensure the detection, prevention, response to, and investigation of cybercrime incidents and misuse of Postal Service information technology assets. Adherence to information security policies will safeguard the integrity, confidentiality, and availability of Postal Service information and protect the interests of its personnel, business partners, and the public.

Adherence to information security policies enables compliance with regulations to which the Postal Service is subject, including Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standards (PCI-DSS). This policy reflects standards and guidelines suggested by industry organizations such as the Public Company Accounting Oversight Board (PCAOB), American Institute of Certified Public Accountants (AICPA), Committee of Sponsoring Organizations (COSO), and National Institute of Standards and Technology (NIST).

Information security policy will ensure the creation and implementation of an environment that:

a. Protects information resources critical to the Postal Service.

b. Protects information as mandated by federal laws, regulations, directives, law enforcement and judicial processes, and industry requirements.

c. Protects the personal information and privacy of employees and customers.

d. Reinforces the reputation of the Postal Service as an institution deserving of public trust.

f. Assigns responsibilities to relevant Postal Service officers, executives, managers, employees, contractors, partners, and vendors.

g. Reviews and revises information security policies and procedures in accordance with evolving security threats.

The following principles guide the development and implementation of Postal Service information security policies and practices:

a. Information is:

- A critical asset that must be protected.
- Restricted to authorized personnel for authorized use.

b. Information security is:

- Cornerstone of maintaining public trust.
- A business issue — not a technology issue.
- Risk based and cost effective.
- Aligned with Postal Service priorities, industry-prudent practices, government requirements, and federal laws.
- Directed by policy but implemented by business owners.
- Everybody's business.

1-2 Scope

Information resources are strategic assets vital to the business performance of the Postal Service. These strategic assets belong to the Postal Service as an organization and not to any individual or group of individuals and must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Postal Service's ability to conduct its mission.

Information security applies to all information resources, organizations, and personnel. Chapter 1 addresses the following:

a. Infrastructure components/systems.

b. Information resources.

c. Organizations and personnel.

d. Importance of compliance.

e. Policy exception and review.

1-3 Policy

The Postal Service information security policies are grouped in the following areas:

a. Security roles and responsibilities.

b. Information designation and control.

c. Security risk management.

d. Acceptable use.

e. Personnel security.

f. Physical and environmental security.

g. Development and operations security.

h. Information security services.

i. Hardware and software security.

j. Corporate network security.

k. Business continuity management.

l. Security incident management.

m. Security compliance and monitoring.

~~Certain~~ Information about individuals that is collected and stored by information resources is subject to the Privacy Act of 1974, as amended (Privacy Act).

The Privacy Act requires all federal agencies, including the Postal Service, to adhere to a minimum set of standards for the collection and storage of certain personal data and ~~restricts~~ limits the disclosure of such Privacy Act information. Agencies are required to establish appropriate administrative, technical, and physical safeguards to protect Privacy Act data. These safeguards ensure the integrity and confidentiality of information resources containing Privacy Act data and protect against unauthorized disclosure of such data, which could result in substantial harm, embarrassment, unfairness, or inconvenience to an individual.

1-4 Supporting Documentation

The following handbooks, management instructions, and contract clauses provide implementation policy and guidelines for this handbook:

a. Handbook AS-805-A, *Information Resource Certification and Accreditation Process.*

b. Handbook AS-805-D, *Information Security Network Connectivity Process.*

c. Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment (MPE/MHE).*

d. Handbook AS-805-H, *Cloud Security.*

e. Management Instruction FM 640-2011-3, *Payment Card Industry Data Security Standard (PCI DSS).*

f. Contract clauses 1-1, Privacy Protection, and 4-19, Information Security Requirements ~~Resource,~~ in the Postal Service's *Supplying Principles and Practices.*

1-5 Policy Owner

The policy owner of this handbook is the manager of the Corporate Information Security Office.

1-6 Infrastructure Components/Systems

1-6.1 General

Infrastructure components/systems are the underlying foundation for information resources and include cyber-based resources (e.g., network hardware and software).

The infrastructure components/systems are usually major groupings or network segments that provide reusable and repeatable services for application systems and are generally considered to be critical components/ systems of the Postal Service computing environment.

An infrastructure component/system typically does the following:

a. The system is typically an ~~underlining~~ underlying part of the Postal Service network environment.

b. The system does not provide a direct user interface and multiple user functionality.

c. The system provides reusable and repeatable services for multiple applications.

d. The system does not typically require periodic code changes or ~~/~~customer acceptance testing, developer intervention or regular upgrades.

1-6.2 External Technology Solutions

External technology solution types are categorized as follows:

a. Service-based contract solution.

b. Hosted solution.

c. Cloud solution.

1-6.2.1 Service-Based Contract Solution

A service-based contract solution is required for a company that is providing a service to the Postal Service such as financial services (Wells Fargo), Licensee (NCOA Link, Stamp reseller), and Inter-Agency Agreements. A service-based contract is different from other external technology solutions in that the service provider has custody of USPS data and is responsible for:

a. Protecting Postal Service data.

b. All aspects of its security (e.g., physical, personnel, network, application).

c. Mitigating and reporting incidents such as breaches.

1-6.2.2 Hosted Solution

A hosted solution requires the business partner to host a separate instance of an application for Postal Service use. The business partner typically owns or leases the physical servers used in the solution and the servers utilized for Postal Service are not shared with anyone else. Data storage and backup requires segregation through encryption and physical or logical isolation/ separation based on data classification.

1-6.2.3 Cloud Solution

A cloud solution enables network access to a shared pool of configurable virtualized computing resources (e.g., networks, servers, storage, applications, and services) in which information technology enabled capabilities are delivered "as a service" to multiple customers using the same computing resources. The cloud environment can be rapidly scaled up or down and tailored to serve multiple consumers on demand with minimal management effort or service provider interaction.

Cloud solutions must not be confused with [1] hosted solutions that are managed and maintained by the supplier and provide physical separation of the hardware that is leased, purchased or isolated for the exclusive use of Postal Service or [2] service-based contracts where the supplier takes ownership and full responsibility for the security of the data.

Data must not be viewed, processed, transmitted, or stored outside the United States (including U.S. territories). See Handbook AS-805-H for additional cloud security requirements.

1-6.3 External Technology Solution Security and Privacy Assessments

1-6.3.1 Service-Based Contract Solution Security and Privacy Assessment

To determine how the service provider will protect Postal Service data, all service-based contract solutions must be evaluated by Corporate Information Security (CISO) and the Privacy Office to evaluate the service provider's protection posture. This evaluation will include, but is not limited to a review of the service provider's internal documentation as well any third-party assessment documentation that can assist in verifying third-party control implementation, such as, ISO 27001, SOC2, ~~and~~ PCI DSS, NIST/FedRAMP.

1-6.3.2 Cloud and Hosted Solution Security and Privacy Assessment

To determine how the solution provider will protect Postal Service data:

a. The offsite hosting letter must be reviewed and approved by CISO and Privacy Office.

b. All hosted and cloud solutions must complete the USPS ~~infrastructure security assessment process.~~ Certification and Accreditation process.

1-6.3.3 Cloud Solution Security and Privacy Assessment

All cloud solutions collecting, transmitting, or storing sensitive or sensitive-enhanced (including PII, PCI, and law enforcement) data must complete and maintain a current FedRAMP Authorization as guided by the AS

805Hcertification. If FedRAMP certification is in process an interim Unless otherwise stated in the contract with the CSP, a security assessment will be conducted using the Postal Service infrastructure security assessmentCertification and processAccreditation process.

All cloud solutions that are non-sensitive and non-criticalregardless of sensitivity and criticality, will utilize the Postal Service infrastructure security assessmentCertification and Accreditation process if not already FedRAMPto evaluated. the risk regardless of the FedRAMP status. If the solution has been FedRAMP evaluated, CISO will assess that evaluation.

1-7 Information Resources

Information security policies apply to all information, in any form, related to Postal Service business activities, employees, or customers that have been created, acquired, or disseminated using Postal Service resources, brand, or funding. Information security policies apply to all technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information. Information security policies also apply to all information systems, infrastructure, applications, products, services, telecommunications networks, computer-controlled mail processing equipment, and related resources, which are sponsored by, operated on behalf of, or developed for the benefit of the Postal Service.

Exhibit 1-7 shows examples of information technologies and the information they contain that are collectively known as information resources. Information resources may be referred to as technology solutions within the Technical Solutions Life Cycle (TSLC).

Exhibit 1-7
Examples of Information Resources

Category	Description	Examples
Systems and Equipment	All multi-user computers and computer controlled systems and their components.	■ Data Processing ■ Automated Information Systems (AIS) ■ Process Control Computers ■ Process Control Systems ■ Embedded Computer Systems ■ Mainframe Computers ■ Minicomputers ■ Microcomputers ■ Microprocessors ■ Office Automation Systems ■ Stand-Alone, Shared Logic, or Shared Resource Systems ■ Firmware ■ Servers ■ Kiosks ■ Intelligent Vending Machines

Mail Processing Equipment (MPE)	All computer-controlled equipment and networks used in processing, distributing, and transporting the mail.	■ Bar Code Sorters ■ Flat Sorters ■ Optical Character Readers ■ Data Collection System ■ Routers and Switches ■ Tray Management System ■ Forwarding Control System ■ MPE Support System

Category	**Description**	**Examples**
Single-User Computer Equipment	All computers and their components used by individuals.	■ Personal Computers (PCs) ■ Workstations ■ Mobile Computing Devices – Laptop Computers – Notebook Computers – Tablet Devices – Phablets – Handheld Computers – Smart Phones – Scanners
Hardware	All major items of equipment or their components associated with a computer system.	■ Central Processing Units (CPUs) ■ Random Access Memory (RAM) ■ Hard Drives ■ Network Interface Cards ■ Terminals ■ Monitors ■ Speakers ■ Video Display Terminals ■ Projection Equipment ■ Modems ■ Printers ■ Scanners
Software	All programs, scripts, applications, operating systems, HTML, and related resources.	■ Operating Systems (OS) ■ Programs (Source and Object) ■ Applications ■ Applets ■ Macros, Scripts ■ Database Management Systems ■ Custom Code ■ Associated Documentation
Data and Information	All information or data stored in digital format, or as a printed product of data stored in digital format.	■ Text Files ■ Documents ■ Spreadsheets ■ Digital Images ■ Electronic Mail ■ Tables ■ Databases ■ Biometrics Information

Products and Services	All objects, processes, functions, and information delivered by, for, or under the brand of the Postal Service.	■ Information Delivery Services ■ E-Commerce Applications ■ Digital Certificate Services ■ Web Site Content ■ Managed Services

Category	Description	Examples
Network Facilities	All communications lines and associated interconnected communications equipment.	■ Transition Lines ■ Terminal Equipment ■ Routers ■ Firewalls ■ Hubs ■ Switches ■ Local Area Networks (LANs) ■ Wide Area Networks (WANs) ■ Virtual Private Networks (VPNs) ■ Infrastructure ■ Internet ■ Intranet ■ Extranet ■ Telephone and Telephone Systems ■ Voice-Messaging Systems ■ Fax Machines ■ Videoconferencing Equipment ■ Wireless Communications
Media	All electronic and non-electronic media used for information exchange.	■ Magnetic Tapes ■ Magnetic or Optical Disks ■ Diskettes ■ USB Devices ■ Hard-Copy Printouts

1-8 Organizations and Personnel

Information security policies apply to all Postal Service functional organizations and personnel, including Postal Service employees, contractors, vendors, suppliers, business partners, and any other authorized users of Postal Service information systems, applications, telecommunication networks, data, and related resources, regardless of location. Information security applies to the Office of the Inspector General and the Inspection Service except where statutory authority exempts them.

For the purposes of these policies, the above entities are collectively known as personnel. This definition of "personnel" excludes customers whose only access is through publicly available services, such as public Web sites of the Postal Service.

These policies do not change the rights or responsibilities of either management or the unions pursuant to Articles 17 and 31 of the various

collective bargaining agreements or the National Labor Relations Act, as amended. These revisions do not bar the unions from using their own portable devices and media for processing information that is relevant for collective bargaining and/or grievance processing, including information provided by management pursuant to Articles 17 and 31 of the collective bargaining agreement or the National Labor Relations Act. There is no change to policy concerning restricted access to the Postal Service Intranet.

Note: For specific guidance regarding practices or actions not explicitly covered by these policies, contact the manager, Corporate Information Security Office, prior to engaging in such activities.

1-9 Importance of Compliance

1-9.1 Maintaining Public Trust

The public entrusts vast amounts of information to the Postal Service every day — information that the Postal Service is required by law and good business practice to protect. Compliance with information security policies will help protect information resources and enhance the reputation of the Postal Service as deserving of public trust.

1-9.2 Continuing Business Operations

The Postal Service is committed to delivering superior customer service in an increasingly competitive marketplace through the effective use of technology, information, and automation. Compliance with information security policies will help ensure the continuous availability and integrity of the technological infrastructure that is critical to the Postal Service's ability to perform its mission.

1-9.3 Protecting Postal Service Investment

Postal Service information resources represent a sizable financial investment in technologies and in information that can never be replicated. These information resources are of paramount importance to the mission of the Postal Service and to the country and must be protected.

1-9.4 Abiding by Federal Regulations

Postal Service information security policies are designed to respond to the intent and spirit of government laws, regulations, and directives.

1-10 Policy Exception and Review

1-10.1 Granting an Exception to the Policies

Any exception to the policies in this handbook must be based on a completed risk assessment and documented in a risk acceptance letter approved by the vice president, Information Technology, and the vice president of the function business area. (Risk acceptance is defined in 4-6, Risk-Based Information Security Framework, of this handbook). If the exception impacts sensitive or sensitive-enhanced information, the Chief Privacy Officer (CPO) must also approve the exception. (Information categories and levels are defined in 3-2, Information Designation and Categorization, of this handbook).

1-10.2 Policy Review

Information security policy is reviewed on semiannual basis and updated as needed to reflect changes to business objectives, government, and industry requirements, and risks to the computing environment. A call for updates is sent to applicable Postal Service organizations. Comments, suggestions, and recommended changes are submitted to the Corporate Information Security Office (CISO).

Organizations can submit suggestions and recommended changes to CISO anytime throughout the year, as the need arises. All comments, suggestions, and recommended changes are reviewed by the CISO for possible inclusion in information security policy documents.

The CISO responds to the submitter with a summary of the action to be taken. Approved changes are packaged into a draft change document which is then vetted with Postal Service organizations. The CISO reviews all comments received from the vetting process against federal laws, regulations, directives, circulars, memoranda, and standards; industry standards and best practices; and Postal Service business needs. The finalized change document is submitted for signoff by the chief security officer and for publication on PolicyNet.

2 Security Roles and Responsibilities

2-1 Policy

Information security is the individual and collective responsibility of all Postal Service personnel, business partners, and other authorized users. Access to information resources is based on an individual's roles and responsibilities. Only authorized personnel are approved for access to Postal Service information resources.

All information technology managers are responsible for securing the Postal Service computing environment, which includes information resources and infrastructure, by implementing appropriate technical and operational security processes and practices that comply with Postal Service information security policies.

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for implementing information security policies. All officers and managers must ensure compliance with information security policies by organizations and information resources under their direction and provide the personnel, financial, and physical resources required to appropriately protect information resources.

All Postal Service personnel are responsible for complying with all Postal Service information security policies.

2-2 Consolidated Roles and Responsibilities

2-2.1 Chief Information Officer and Executive Vice President

The chief information officer (CIO) and executive vice president is responsible for the following:

a. Acting as the senior information technology (IT) decision maker and corporate change agent to securely integrate the key components of business transformation: technology, processes, and people.

b. Providing advice and assistance to senior managers on information security policy and their compliance-based performance.

c. Promoting the implementation of an information security architecture to mitigate information security-related risk.

d. Promoting the protection of corporate information resources across Postal Service organizations and business partners.

e. Together with the vice president of the functional business area (data steward) and chief privacy officer (CPO), approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. If this responsibility is delegated, notice to that effect must be writing. See 3-5.5.

2-2.2 Chief Postal Inspector

The chief postal inspector is responsible for the following:

a. Establishing policies, procedures, standards, and requirements for personnel, physical, and environmental security.

b. Approving the identification of sensitive positions.

c. Conducting background investigations and granting personnel clearances.

d. Conducting site security reviews, surveys, and investigations of facilities containing Postal Service computer and telecommunications equipment to evaluate all aspects of physical, environmental, and personnel security.

e. Providing technical guidance on physical and environmental security activities that support information security, such as controlled areas, access lists, physical access control systems, and identification badges; providing protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

f. Providing security consultation and guidance during system, application, and product development to assure that security concerns are addressed and information and/or evidence that may be needed for an investigation is retained by the information resource.

g. Assisting the manager, Corporate Information Security Office (CISO), with reviews, as appropriate.

h. Investigating reported security incidents and violations.

i. Conducting revenue/financial investigations including theft, embezzlement, or fraudulent activity.

j. Providing physical protection and containment assistance and investigating information security incidents as appropriate.

k. Funding CISO investigative efforts outside of those normally required.

l. Managing, securing, scanning, and monitoring the Inspection Service's network and information technology infrastructure.

m. Defining high-risk international destinations where personnel are prohibited from traveling with their standard issue Postal Service computers and communications equipment (including laptops, notebook computers, external hard drives, ~~Blackberry~~ mobile devices, Universal Serial Bus (USB) devices, etc.).

n. Providing temporary equipment to use when traveling to high-risk international destinations.

2-2.3 Vice President, Information Technology

The vice president, Information Technology (IT), is responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of information processed by IT applications.

c. Ensuring compliance with the information security certification and accreditation processes.

d. Together with the vice president of the functional business area, accepting, in writing, residual risks of information resources under their control. The VP IT may delegate this authority to the applicable Business Relationship Management manager. If this authority is delegated, notice to that effect must be in writing.

e. Reporting to senior management on the status of an incident with a major IT application.

f. Defining and documenting secure coding best practices.

2-2.4 Manager, Computer Operations

The manager of Computer Operations is responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of information processed at IT sites.

c. Ensuring the protection and secure implementation of the Postal Service IT infrastructure.

d. Supporting the information security certification and accreditation processes.

e. Together with the vice president of the functional business area (data steward) and CPO, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from an IT facility. (If this responsibility is delegated, notice to that effect must be writing. See 3-5.5.)

f. Reporting to senior management on the status of an incident at a major
IT facility.

g. Reviewing and utilizing C&A documentation in the IT Artifacts Library.

h. Resolving identified vulnerabilities.

2-2.5 Chief Information Security Officer

The chief information security officer (CISO) is responsible for the following:

a. Setting the overall strategic and operational direction of the Postal Service information security program and the program's implementation strategies.

b. Engaging at any point on any level for issues related to information security that impact the Postal Service.

c. Recommending members to the ~~Information Security~~ Executive Cyber Risk Committee (ECRC)~~Council~~.

d. Developing and disseminating information security policies, processes, standards, and procedures.

e. Managing the certification and accreditation (C&A) process.

f. Providing guidance on application security, reviewing the C&A documentation package, and accrediting sensitive-enhanced, sensitive, and critical information resources developed for, endorsed by, or operated on behalf of the Postal Service.

g. Managing the Network Change Review Board (NCRB) process.

h. Authorizing temporary access to information resource services.

i. Conducting site security reviews or providing support to the Postal Inspection Service during its site security reviews, as requested.

j. Providing consulting support for securing the network perimeter, infrastructure, integrity controls, asset inventory, identification, authentication, authorization, intrusion detection, penetration testing, and audit logs and for information security architecture, technologies, procedures, and controls.

k. Approving encryption technologies.

l. Providing leadership of the security initiatives for the Enterprise Architecture Forum.

m. Developing and implementing a comprehensive information security training and awareness program that is mandatory for all employees at time of hire and annually thereafter.

n. Serving as the central point of contact for all information security issues and providing overall consultation and advice on information security policies, processes, standards, procedures, requirements, controls, services, and issues.

o. At least semiannually, assessing the adequacy of information security policy and process to reflect changes to business objectives and the operating environment (including technology infrastructure, threats, vulnerabilities, and risks).

p. At least annually, assessing the adequacy of information security controls and recommending changes as necessary.

q. Establishing evaluation criteria and recommending security hardware, software, and audit tools.

r. Approving the establishment of shared accounts.

s. Ensuring compliance to information security policies and standards through inspections, reviews, and evaluations.

t. Providing support to the Office of the Inspector General (OIG) and the Inspection Service during the conduct of investigative activities concerning information security, the computing infrastructure, and network intrusions, as requested.

u. Providing support to the chief postal inspector during the conduct of facility/site security reviews, as requested.

v. Escalating security issues to executive management and promulgating security issues and recommended corrective actions across the Postal Service.

w. Authorizing monitoring and surveillance activities of information resources.

x. Authorizing (in case of threats to the Postal Service infrastructure, network, or operations) appropriate actions that may include viewing and/or disclosing data to protect Postal Service resources or the nation's communications infrastructure.

y. Confiscating and removing any information resource suspected of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be used in forensic analysis of a security incident.

z. Reviewing and approving information security policy for mail processing equipment/mail-handling equipment (MPE/MHE).

aa. Providing guidance and program direction for security solutions, and ensuring adherence of the solution to the existing policies.

2-2.6 ~~Information Security Executive Council~~Enterprise Executive Cyber Risk Committee

~~The Information Security Executive Council consists of appropriate Postal Service representatives and serves as a steering committee advising the CISO and promulgating information security throughout the Postal Service.~~

The purpose of the Executive Cyber Risk Committee (ECRC) is to establish, communicate, and regularly review the USPS cyber risk capacity and appetite and keep the Postmaster General abreast of cyber risks that may impact the cyber network.

2-2.7 Vice Presidents, Functional Business Areas

The vice presidents of Postal Service functional business areas are responsible for the following:

a. Ensuring resources are available for completing information security tasks.

b. Ensuring the security of all information resources within their organization.

c. Together with the VP IT, accepting, in writing, residual risks of information resources under their control. The vice presidents of functional business areas may delegate this authority to the

applicable executive sponsor. If this authority is delegated, notice to that effect must be in writing.

d. Ensuring that contractual agreements require all suppliers, contractors, vendors, and business partners under each VP's purview to adhere to Postal Service information security policies.

e. Together with the CIO and CPO, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. (If this responsibility is delegated, the delegation of responsibility must be writing.)

~~e.~~f. Oversee organizational compliance for regulatory and external requirements (SOX, PCI).

2-2.8 Vice President, Engineering

a. The vice president, Engineering Systems, is responsible for ensuring the security of information resources used in support of the MPE/MHE environment, including technology acquisition, development, and maintenance.

~~a.~~b. Oversee organizational compliance for regulatory and external requirements (SOX, PCI)

2-2.9 Vice President, Network Operations

The vice president, Network Operations, is responsible for the security of the mail and information resources used in support of strategies and logistics.

2-2.10 Officers and Managers

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for the following:

a. Implementing information security policies, ensuring compliance with information security policies by organizations and information resources under their direction, and invoking user sanctions as required.

b. Identifying sensitive information positions in their organizations and ensuring that personnel occupying sensitive positions hold the appropriate level of clearance.

c. Managing access authorizations and documenting information security responsibilities for all personnel under their supervision.

d. Ensuring all personnel under their supervision receive information security training commensurate with their responsibilities upon hire and annually thereafter, and maintaining auditable training records when there isn't an automated system.

e. Ensuring all personnel under their supervision comply with Postal Service information security policies and procedures.

f. Including employee information security performance in performance evaluations.

g. Supervising information security responsibilities of their onsite contractor personnel.

h. Processing departing personnel appropriately and notifying the appropriate system and database administrators when personnel no longer require access to information resources.

i. Initiating a written request for message data content or Internet usage monitoring and sending it to the CPO for approval.

j. Approving or denying requests, by personnel under their supervision, for access to information resources beyond temporary information resource services and reviewing those access authorizations on a semiannual basis.

k. Ensuring that all hardware and software are obtained in accordance with official Postal Service processes.

l. Protecting information resources and ensuring their availability through business continuity activities including plans, procedures, off-site backups, periodic testing, workarounds, and training/cross-training essential and alternate personnel.

m. Ensuring that personnel under their supervision who remove a portable electronic device or media from a Postal Service facility are aware of their responsibility for its security and have a place to secure the device or media when it is not being used.

n. Ensuring compliance with Postal Service information security policy and procedures.

o. Reporting suspected information security incidents to CyberSafe immediately, protecting information resources at risk during security incidents, containing the incident, and following continuity plans for disruptive incidents (see Chapter 13, Security Incident Management).

2-2.11 Executive Sponsors

Executive sponsors, as representatives of the vice president of the functional business area, are the business managers with oversight (e.g., funding, development, production, and maintenance) of the information resource and are responsible for the following:

a. Consulting with the CPO for determining information sensitivity and Privacy Act applicability.

b. Ensuring a business impact assessment (BIA) is conducted to determine the sensitivity and criticality of each information resource under his or her control and to determine the potential consequences of information resource unavailability.

c. Providing resources to ensure that security requirements are properly addressed and information resources are properly protected.

d. Ensuring completion of a site security review, if the facility hosts an information resource designated as sensitive-enhanced, sensitive, or critical.

e. Ensuring that contract personnel under their supervision comply with Postal Service information security policies and procedures.

f. Ensuring that all information security requirements are included in contracts and strategic alliances.

g. Ensuring compliance with and implementation of the Postal Service privacy policy; data collection, retention, and destruction policies; customer or employee privacy notices; and software licensing.

h. Appointing, in writing, an information systems security representative (ISSR).

i. Ensuring completion of security-related activities throughout the Information resource C&A life cycle.

j. Ensuring that information resources within their purview are capable of enforcing appropriate levels of information security services to ensure data integrity.

k. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.

l. Authorizing access to the information resources under their control and reviewing those access authorizations on a semiannual basis.

m. Maintaining an accurate inventory of Postal Service information resources and coordinating hardware and software upgrades.

n. Ensuring appropriate funding for proposed business partner connectivity, including costs associated with the continued support for the life of the connection.

o. Initiating and complying with the network connectivity request requirements and process as documented in the Information Security Network Connectivity Process.

p. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

q. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

r. Funding application recovery (including but not limited to hardware/ software licenses required, continuity plan development, testing, and maintenance) for applications.

s. If the VP functional business area delegated this authority to the executive sponsor, the executive sponsor will work jointly with the VP IT (or the Business Relationship Management manager if this authority is delegated) to review the C&A documentation package, accept the residual risk to an application, and approve the application for production or return the application to the applicable life cycle phase for rework.

t. Reporting suspected information security incidents to CyberSafe immediately, protecting information resources at risk during the security incident, containing the incident, and following continuity plans for disruptive incidents.

u. Coordinating the resolution of identified vulnerabilities with the appropriate IT organization (e.g., Computer Operations, Business Relationship Management, Solutions Development and Support, etc.).

2-2.12 Functional System Coordinators

The functional system coordinator (FSC) role is an ad hoc activity assigned by a data steward and is not a position or job function. An FSC has expert knowledge of the information resource and is familiar with the people and levels of access being requested. The FSC role may be required for all information resources registered in ~~eAccess~~ARIS~~e~~Access/ARIS. The FSC role is restricted to authorized Postal Service employees and contractors.

An FSC is responsible for approving or denying a request based on the role or access level requested. If access to an information system is requested, the FSC is responsible for ensuring that the requestor has successfully completed the appropriate background investigation or obtained the appropriate clearance. The FSC has the last level of approval before a request is sent to the log-on administrator to create the account, which will then become active.

2-2.13 Business Relationship Management Portfolio Managers (formerly Portfolio Managers)

Business Relationship Management portfolio managers are responsible for the following:

a. Supporting the executive sponsor in the development of information resources and the C&A process, including the BIA, risk assessment, and business continuity plans.

b. If an ISSR has not been assigned by the executive sponsor, appointing an ISSR to perform security-related activities.

c. Providing coordination and support to executive sponsors and disaster recovery (DR) service providers for all matters relating to business continuity planning.

d. Reviewing the C&A documentation package and completing a risk mitigation plan for risks identified as high or medium. If a documented high or medium vulnerability will not be mitigated, preparing and signing a Risk Acceptance Letter as part of the C&A process.

e. Business Relationship Management portfolio managers are responsible for the following: If the VP IT delegated this authority to the Business Relationship Management portfolio manager, the Business Relationship Management portfolio managers will work jointly with the vice president of the functional business area (or the executive sponsor, if this authority is delegated) to review the C&A documentation package, accept the residual risk to an information resource, and approve the information resource for production or return the information resource to the applicable life-cycle phase for rework.

f. Ensuring that the information resource is registered in ~~eAccessARISe~~Access/ARIS.

g. Accepting personal accountability for adverse consequences if the information resource was placed in production before the C&A process was completed.

h. Managing projects through their project managers who are responsible for the following:

(1) Incorporating the appropriate security controls in all information resources.

(2) Developing and maintaining C&A documentation as required.

(3) Ensuring that the information resource is entered in the Enterprise Information Repository (EIR) and updated as required.

(4) Filing C&A documentation in the IT Artifacts Library and maintaining the hardcopies and electronic copies for the appropriate retention periods.

i. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

j. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

k. Completing along with their staff the annual C&A training.

l. Resolving identified vulnerabilities.

2-2.14 Managers of Information Technology Solution Centers

The managers of Information Technology Solution Centers are responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of data.

c. Ensuring the protection and secure implementation of the Postal Service IT infrastructure.

d. Ensuring compliance with the information security C&A processes.

e. Together with the vice president of the functional business area, accepting, in writing, residual risk of applications and approving deployment.

f. Together with the vice president of the functional business area, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. (If this responsibility is delegated, notice to that effect must be writing.)

g. Managing projects through their project managers who are responsible for the following:

(1) Incorporating the appropriate security controls in all information resources.

(2) Developing C&A documentation as required.

(3) Ensuring that the information resource is entered in the Enterprise Information Repository (EIR) and updated as required.

(4) Filing C&A documentation in the IT Artifacts Library and maintaining the hardcopies and electronic copies for the appropriate retention periods.

h. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

i. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

j. Functioning as the incident management team leader for their facility.

k. Identifying and training key technical personnel to provide support in business continuity planning for their facility, information resources housed in their facility, and the alternate DR facilities.

l. Resolving identified vulnerabilities.

2-2.15 Installation Heads

Installation heads are in charge of Postal Service facilities or organizations, such as areas, districts, Post Offices, mail processing facilities, parts depots, vehicle maintenance facilities, computer service centers, or other installations. Installation heads are responsible for the following:

a. Designating a security control officer (SCO) who is responsible for personnel and physical security at that facility, including the physical protection of computer systems, equipment, and information located therein.

b. Implementing physical and environmental security support for information security, such as the protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

c. Controlling physical access to the facility, including the establishment and implementation of controlled areas, access lists, physical access control systems, and identification badges.

d. Funding building security equipment and security-related building modifications.

e. Maintaining an accurate inventory of Postal Service information resources at their facilities and implementing appropriate hardware security and configuration management.

f. Maintaining and upgrading all security investigative equipment, as necessary.

g. Ensuring completion of a site security review, providing assistance to the Inspection Service and CISO as required, and accepting site residual risk.

h. Ensuring that the Postal Service security policy, standards, and procedures are followed in all activities related to information resources (including procurement, development, and operation) at their facility.

i. Ensuring that all employees who use or are associated with the information resources in the facility are provided information security training commensurate with their responsibilities and taking appropriate action in response to employees who violate established security policy or procedures.

j. Cooperating with the Inspection Service to ensure the physical protection of the network infrastructure located at the facility.

k. Developing, maintaining, and testing:

(1) Emergency Action Plans required for each facility to ensure personnel are safely evacuated and provides for the protection of the employees.

(2) Incident Management Facility Recovery Plan required for each major IT site.

(3) Workgroup Recovery Plan required for each business function.

(4) Disaster Recovery Plan (DRP) (business information systems disaster) documents required for each critical system that supports essential (core) business functions.

i Implementing and managing the following plans and team members:

(1) Emergency Action Plan.

(2) Incident Management Facility Recovery Plan.

(3) Workgroup Recovery and "Beyond" Continuity of Operations (COOP) Plans.

(4) DRP (business information systems disaster) documents.

i. Reporting information security incidents to CyberSafe immediately, containing the incident, following continuity plans for disruptive incidents, and assessing damage caused by the incident.

j. Resolving identified vulnerabilities.

2-2.16 Chief Privacy Officer

The CPO is responsible for the following:

a. Developing policy for defining information sensitivity and determining information sensitivity designations.

b. Providing guidance on privacy issues to ensure Postal Service compliance with the Privacy Act, the Freedom of Information Act, Gramm-Leach-Bliley Act, and Children's Online Privacy Protection Act.

c. Developing privacy compliance standards, customer or employee privacy notices, and customer data collection standards, including cookies and Web-transfer notifications.

d. Developing appropriate data record retention, disposal, and release procedures and standards.

e. Approving requests for message data content or Internet usage monitoring.

f. Consulting on and reviewing the BIA and approving the determination of information sensitivity.

g. Providing guidance throughout the investigation of a mass data compromise relating to the privacy of customer and employee/ contractor personal information.

h. Developing communications to transmit to impacted parties to a mass data compromise.

2-2.17 Inspector General

The inspector general is responsible for the following:

a. Conducting independent financial audits and evaluation of the operation of the Postal Service to ensure that its assets and resources are fully protected.

b. Preventing, detecting, and reporting fraud, waste, and program abuse.

c. Investigating computer intrusions and attacks against Postal Service information resources per agreement with the Inspection Service.

d. Investigating the release or attempted release of malicious code onto Postal Service information resources.

e. Investigating use of Postal Service information resources to attack external networks.

f. Promoting efficiency in the operation of the Postal Service.

g. Funding CISO investigative efforts outside of those normally required.

h. The manager, Technical Crimes Unit (TCU), is responsible for the following:

(1) Functioning as an ongoing liaison with CyberSafe.

(2) Serving as a point of contact between CyberSafe and law enforcement agencies.

(3) Conducting criminal investigations of attacks upon Postal Service networks and computers.

2-2.18 Manager, Business Continuance Management

The manager, Business Continuance Management, is responsible for the following:

a. Protecting the health and safety of Postal Service employees.

b. Ensuring the continuity of business, expediting recovery from a loss of a single critical system or a major disruption to business functions.

c. Reviewing and assessing Business Continuity Management (BCM) program plans.

d. Defining, planning, developing, implementing, managing, assuring the testing and exercising, and monitoring for compliance of a sustainable BCM program for the Postal Service.

e. Ensuring appropriate Business Continuity Plans (BCPs) are developed, tested, and exercised for business functions and information technology services.

f. Ensuring appropriate DRP documents are developed and business information systems are tested for all critical and business functions and services.

g. Certifying all DRP test and BCP exercise.

h. Developing and implementing lines of communication to the IT organization about BCM matters.

i. Promoting BCM awareness and providing training for Postal Service personnel.

j. Ensuring compliance with BCM and information security policies.

k. Establishing BCM policy and strategy.

2-2.19 Manager, Telecommunications Services

The manager, Telecommunications Services (TS), is responsible for the following:

a. Implementing and maintaining operational information security throughout the network infrastructure including timely security patch management. Critical security patches for PCI-related information resources must be installed within 30 days of release.

b. Recommending and deploying network hardware and software based on the Postal Service security architecture.

c. Operational monitoring and tracking of all physical connections between any component of the Postal Service telecommunications infrastructure and any associated information resource not under Postal Service control.

d. Implementing security controls and processes to safeguard the availability and integrity of the Postal Service intranet including physical access to network infrastructure and the confidentiality of sensitive-enhanced and sensitive information.

e. Implementing the network perimeter firewalls, demilitarized zones, secure enclaves, and proxy servers.

f. Designating TS representative(s) to the NCRB.

g. Ensuring secure and appropriate connectivity to the Postal Service intranet.

h. Ensuring network services and protocols used by Postal Service information resources provide the appropriate level of security for the Postal Service intranet and the information transmitted.

i. Implementing secure methods of remote access and appropriate remote access controls.

j. Implementing two-factor authentication and the associated infrastructure for network management.

k. Implementing only Postal Service-approved encryption technology.

l. Implementing appropriate network security administration and managing accounts appropriately.

m. Maintaining the integrity of data and network information resources.

n. Supporting the implementation of approved security incident detection and prevention technologies (e.g., virus scanning, intrusion detection systems, and intrusion prevention systems) throughout the perimeter.

o. Maintaining an accurate inventory of Postal Service network information resources.

p. Monitoring network security alerts and logs and providing network security audit logs to the CISO ISS.

q. Ensuring that recovery plans and sufficient capacity are in place for the recovery of the telecommunications infrastructure for the IT-supported Postal Service sites.

r. Identifying and training key technical personnel to provide support in BCM for information resources housed in IT-supported Postal Service sites.

s. Monitoring network traffic for anomalies, conducting perimeter scanning for viruses, malicious code, and usage of nonstandard network protocols, and immediately reporting suspected information security incidents to CyberSafe.

t. Protecting information resources at risk during security incidents (if feasible) and providing support for CyberSafe incident containment and response.

u. Approving all wireless technology before any implementation activities are initiated.

v. Implementing and managing wireless local area network connectivity.

w. Detecting unauthorized access points.

x. Resolving identified vulnerabilities.

2-2.20 Managers Responsible for Computing Operations

The managers responsible for computing operations are responsible for the following:

a. Implementing information security policies, procedures, and standards and ensuring compliance.

b. Coordinating and implementing standard platform configurations based on the Postal Service security architecture.

c. Creating and maintaining a timely patch management process and deploying patches to resources under their control. Critical security patches for PCI-related information resources must be installed within 30 days of release.

d. Maintaining an accurate inventory of Postal Service information resources, tracking and reacting to security vulnerability alerts, coordinating hardware and software upgrades, and maintaining appropriate records.

e. Deploying and maintaining anti-virus software and recognition patterns to scan for malicious code and usage of nonstandard network protocols.

f. Supporting the C&A process for internally managed information resources.

g. Ensuring that remote access is appropriately managed.

h. Implementing appropriate security administration and ensuring that accounts are managed appropriately.

i. Maintaining the integrity of data and information resources and ensuring the appropriate level of information resource availability.

j. Ensuring the installation of the authorized internal warning banner (see Exhibit 14-3.3).

k. Disseminating security awareness and warning advisories to local users.

l. Reporting suspected information security incidents to CyberSafe immediately, protecting information resources at risk during security incidents, implementing containment, and assisting in restoring information resources following an attack.

m. Resolving identified vulnerabilities.

2-2.21 Manager, Corporate Information Security Office Information Systems Security

The manager, CISO ISS is responsible for the following:

a. Determining the requirements and standards for secure enclaves.

b. Assessing information resources to determine the need for placement in a secure enclave.

c. Provide oversight for standard configurations and hardening standards in collaboration with MPE/MHE System owners.

d. Approving two-factor authentication (e.g., digital certificates, digital signatures, biometrics, smart cards, and tokens) and the associated infrastructure for network management.

e. Approving and managing intrusion detection systems and intrusion prevention systems.

f. Approving, managing, and ensuring appropriate perimeter penetration testing and network vulnerability scans and testing.

g. Providing support to the OIG during the conduct of investigative activities concerning information security, the computing infrastructures, and network intrusion as requested.

h. Approving the use of networking monitoring tools, except those used by the OIG.

i. Providing support to the chief postal inspector during his or her conduct of site security reviews as requested.

j. Conducting monitoring and surveillance activities.

k. Collecting, correlating, and reviewing all Postal Service security audit log files and security alerts.

l. Reviewing information security policy and processes for MPE/MHE.

m. Developing and maintaining an information security architecture and coordinating a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.

n. Removing network connectivity from any computing device that does not meet the defined operating system and anti-virus software and recognition pattern thresholds.

o. Managing the NCRB to control connectivity to the Postal Service computing infrastructure.

p. Designating the chairperson of the NCRB and additional ISS representative(s) to the NCRB, as required.

q. Designating an information security policy and process program manager who is responsible for establishing, documenting, and disseminating information security policies, standards, and processes.

The manager, NCRB is responsible for the following:

a. Ensuring connectivity requests are submitted in the established format and sufficient in detail to be evaluated properly.

b. Contacting the submitter or technical contact for any additional or missing information.

c. Forwarding the approved connectivity request to the implementation organizations.

d. Providing technical guidance throughout the network connectivity process.

e. Analyzing business cases and supporting documents for connectivity requests.

f. Evaluating connectivity requests and approving or rejecting them based on existing policy and industry leading best practices.

g. Evaluating connectivity requests for Postal Service information resource to secure enclave needs.

h. Assisting the submitter in identifying alternative solutions for rejected requests that are acceptable to the submitter and comply with the Postal Service standards.

i. Reviewing new information resource, infrastructure, and network connections and their effects on overall Postal Service operations and information security.

j. Ensuring all changes made for an emergency request are annotated and submitted via the NCRB process as soon as work is complete.

k. Enforcing standard connectivity and documentation criteria to expedite approval of connectivity requests.

l. Determining criteria for standard connectivity that will allow for preapproved requests.

m. Ensuring compliance with Postal Service information system security policies and procedures, resources, and communications standards.

n. Identifying and reporting unauthorized or non-compliant connections in the Postal Service network to responsible parties.

o. Reviewing and monitoring business partner connectivity to ensure appropriate responses in event of a breach

p. Taking ownership of the NCRB process through stages leading up to Telecom Implementation

q. Performing evaluation and endorsement of Google chrome extensions.

r. Conducting regular training of teams new or unfamiliar with current NCRB policy and procedure.

The manager, CyberSafe is responsible for the following:

a. Providing immediate and effective response not to be restricted to including removal of malware infected device, but also implementing a recommended solution to the affected system owner to repair and restore functionality.

b. Working with an organization to contain, eradicate, document, and recover following a computer security incident. Coordinating with the stakeholders for incidents involving mail processing equipment.

c. Engaging other Postal Service organizations including, but not limited to, the OIG and Inspection Service.

d. Escalating information security issues to executive management as required.

e. Conducting a post-incident analysis, where appropriate, and recommending preventive actions.

f. Maintaining a repository for documenting, analyzing, and tracking Postal Service security incidents until they are closed.

g. Interfacing with other governmental agencies and private-sector computer incident response centers.

h. Participating in and providing lesson-learned information from information security incidents into ongoing information security awareness and training programs.

i. Developing and documenting processes for incident reporting and management.

j. Providing support to the OIG and the Inspection Service, as requested.

k. Managing CyberSafe to help the Postal Service contain, eradicate, document, and recover following a computer security incident and return to a normal operating state.

2-2.22 Managers, Help Desks

The managers, Help Desks, are responsible for the following:

a. Creating the entry for the problem tracking management system for security incidents reported to the Help Desks.

b. Providing technical assistance for responding to suspected virus incidents reported to the Help Desks.

c. Escalating unresolved suspected virus events to CyberSafe.

2-2.23 Contracting Officers and Contracting Officer Representatives

Contracting officers and contracting officer representatives are responsible for the following:

a. Ensuring that information technology suppliers, contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.

b. Thoroughly vetting service providers for PCI services prior to engagement that includes a risk analysis and documentation to reflect due diligence to the PCI assessor.

c. Updating the PCI Program Management Office (PMO) with status information on service providers for the PCI environment.

d. Verifying that information technology suppliers, vendors, and business partners responsible for storing, processing, or transmitting Postal Service payment card information complete an annual Letter of Attestation providing an acknowledgement of their responsibility for the security of payment card data, under the current PCI DSS.

e. Monitoring service provider PCI compliance at least annually.

f. Verifying that all contracts and business agreements requiring access to Postal Service information resources identify sensitive

positions, specify the clearance levels required for the work, and address appropriate security requirements.

g. Verifying that contracts and business agreements allow monitoring and auditing of any information resource project.

h. Verifying that the security provisions of the contract and business agreements are met.

i. Confirming the employment status and clearance of all contractors who request access to information resources.

j. Verifying all account references, building access, and other privileges are removed for contractor personnel when they are transferred or terminated.

k. Notifying CyberSafe of any security breaches reported to them by the service providers.

l. Directing the supplier to remedy code that is identified by the Executive Sponsor, IT Program Manager and CISO ISSO and taking such contractual action as necessary to enforce contract requirements.

m. In the case the CO/COR oversees a SOX relevant service provider, including PC Postage and/or meter vendors, the CO/COR is responsible for the following:

n.Receiving a System Organization Controls 1 (SOC1) report type II or equivalent report (e.g. FedRAMP, SOC2) if applicable, covering the relevant services provided to the US Postal Service.

o. Communicating with compliance and finance groups, on the cadence as requested by each team to discuss exceptions, issues and reporting

p. ~~Complying with all regulations proposed in the Code of Federal Regulations (CFR) (See 39 CFR Part 501)~~Complying with applicable regulations on the authorization to manufacture and distribute postage evidencing systems. (See 39 CFR Part 501).

~~k.~~g. In the case a third party is a new Postage Evidencing System (PES) provider to the US Postal Service, the party must adhere to the application guidelines proposed in the USPS Postage Evidencing System (PES) provider Applicant Onboarding Guide"

2-2.24 General Counsel

The general counsel is responsible for the following:

a. Ensuring that information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.

b. Ensuring that contracts and agreements allow monitoring and auditing of Postal Service information resource projects.

2-2.25 Business Partners

Business partners may request connectivity to Postal Service network facilities for legitimate business needs. Business partners requesting or using connectivity to Postal Service network facilities are responsible for the following:

a. Initiating a request for connectivity to the Postal Service executive who sponsors the request.

b. Complying with Postal Service network connectivity request (see Handbook AS-805-D, *Information Security Network Connectivity Process)* requirements and process.

c. Abiding by Postal Service information security policies regardless of where the systems are located or who operates them. This also includes strategic alliances.

d. Protecting information resources at risk during security incidents, if feasible.

~~d.~~e. Maintain Chain of Custody for information assets exposed during security incidents, to track the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. To ensure the integrity of the evidence for post-incident review or law enforcement involvement.

~~e.~~f. Reporting information security incidents immediately to CyberSafe, the executive sponsor, and the information systems security officer (ISSO) assigned to their project.

~~f.~~g. Taking action, as directed by CyberSafe, to eradicate the incident, recover from it, and document actions regarding the security incident.

~~g.~~h. Allowing site security reviews by the Postal Inspection Service and CISO.

i. Allowing audits by the OIG.

~~h.~~j. Remediateing deficiencies in their security posture as identified by the CISO Risk team during the Third-Party Cybersecurity Risk Assessments of contract requirements.

2-2.26 Accreditor

The manager, CISO, functions as the accreditor and is responsible for the following:

a. Reviewing the risk mitigation plan and supporting C&A documentation package together with business requirements and relevant Postal Service issues.

b. Escalating security concerns or preparing and signing an accreditation letter that makes one of the following recommendations: accepting the information resource with its existing information security controls, requiring additional security

controls with a timeline to implement, or deferring deployment until information security requirements can be met.

c. Forwarding the accreditation letter and C&A documentation package to the Business Relationship Management manager and executive sponsor.

2-2.27 Certifier

The manager, Security Certification and Accreditation Process, who is appointed by the manager, CISO, functions as the certifier and is responsible for the following:

a. Managing and providing guidance to the ISSOs.

b. Reviewing the C&A evaluation report and the supporting C&A documentation package.

c. Escalating security concerns or preparing and signing a certification letter.

d. Forwarding the certification letter and C&A documentation package to the accreditor.

e. Maintaining an inventory of all information resources that have completed the C&A process.

2-2.28 Security Control Officers

SCOs ensure the general security of the facilities to which they are appointed, including the safety of on-duty personnel and the security of mail, Postal Service funds, property, and records entrusted to them [see the *Administrative Support Manual* (ASM) 271.3, Security Control Officers]. SCOs are responsible for the following:

a. Establishing and maintaining overall physical and environmental security at the facility, with technical guidance from the Inspection Service.

b. Establishing controlled areas within the facility, where required, to protect information resources designated as sensitive-enhanced, sensitive, or critical.

c. Establishing and maintaining access control lists of people who are authorized access to specific controlled areas within the facility.

d. Ensuring positive identification and control of all personnel and visitors in the facility.

e. Ensuring the protection of servers, workstations, portable devices, and information located at the facility.

f. Consulting on the facility COOP plans.

g. Conducting annual facility security reviews using the site security survey provided by the Inspection Service.

h. Reporting suspected information security incidents to CyberSafe and providing support for incident containment and response, as requested.

i. Responding to physical security incidents and reporting physical security incidents to the Inspection Service.

j. Interfacing with CyberSafe, Inspection Service, CISO, or OIG, as required.

2-2.29 Information Systems Security Representatives

ISSRs are appointed in writing by the executive sponsors or the Business Relationship Management portfolio manager and are members of the information resource development or integration teams. The role of the ISSR can be performed in conjunction with other assigned duties. If an ISSR is not assigned, the project manager assumes the role. ISSRs are responsible for the following:

a. Providing support to the executive sponsor and Business Relationship Management portfolio manager, as required.

b. Promoting information security awareness on the project team.

c. Ensuring security controls and processes are implemented.

d. Notifying the executive sponsor, Business Relationship Management portfolio manager, and ISSO of any additional security risks or concerns that emerge during development or acquisition of the information resource.

e. Developing or reviewing security-related documents required by the C&A process as assigned by the executive sponsor or Business Relationship Management portfolio manager.

f. Working with the ISSO to complete the eC&A artifacts in the eC&A system and sending other required artifacts (e.g., TAD, operational training, etc.) or their location (i.e., URL) to the ISSO.

2-2.30 Information Systems Security Officers

ISSOs are responsible for the following:

a. Chairing the C&A team.

b. Ensuring that a BIA is completed for each information resource.

c. Ensuring that the responsible project manager records the sensitivity and criticality designations in EIR.

d. Advising and consulting with executive sponsors, Business Relationship Management portfolio managers, and ISSRs during the BIA process so they know the background for (1) baseline security requirements that apply to all information resources and (2) the security requirements necessary to protect an information resource based on the resource's sensitivity and criticality designation.

e. Recommending security requirements to executive sponsors and Business Relationship Management portfolio managers during the BIA process, based on generally accepted industry practices and the risks associated with the information resource.

f. Providing guidance on how information resources are vulnerable to threats, what controls and countermeasures are appropriate, and the C&A process.

g. Conducting site security reviews or helping the Inspection Service conduct them.

h. Reviewing the C&A documentation package.

i. Preparing and signing the C&A evaluation report and forwarding the evaluation report and C&A documentation to the certifier.

j. Coordinate with the IT SOX program on matters pertaining to the C&A documentation (i.e., Dataflow Mappings, Risk Acceptance Letters, Disaster Recovery Plans) for SOX in-scope applications.

2-2.31 Penetration Testers

Penetration Testing are responsible for performing testing activities at the direction of the CISO and Cybersecurity Risk Management. Additionally, the penetration testers shall complete the following:

a. Perform assessments using a variety of penetration testing tools on applications, infrastructure, and other information resources
b. Liaise on behalf of the CISO Risk Management to work with Business Project Leaders and System owners to gather information in support of penetration testing activities
c. Review findings discovered by penetration testing
d. Assist in planning and support of Red Team activities at the discretion of the CISO Risk Management
e. Ensure that validation related activities are performed in support of Vulnerability Remediation Management Team requirements
f. Informs the CISO Risk Management of any issues impeding progress towards successful penetration testing engagements
g. Compile penetration testing reports for review by CISO Risk Management
h. Provide technical assistance and expertise to CISO pertaining to specific vulnerabilities and findings within the enterprise.

2-2.~~3~~32 System and Network Administrators

System and network administrators are technical personnel who serve as computer systems, network, server, and firewall administrators, whether the system management function is centralized, distributed, subcontracted, or outsourced. System and network administrators are responsible for the following:

a. Implementing information security policies and procedures for all information resources under their control, and also for monitoring the implementation for proper functioning of security mechanisms.

b. Implementing appropriate platform security based on the platform specific hardening standards for the information resources under their control.

c. Complying with standard configuration settings, services, protocols, and change control procedures.

d. Applying approved patches and modifications in accordance with policies and procedures established by the Postal Service. Ensuring that security patches and bug fixes are kept current for resources under their control.

e. Implementing appropriate security administration and ensuring that log-on IDs are unique.

f. Setting up and managing accounts for information resources under their control in accordance with policies and procedures established by the Postal Service.

g. Disabling accounts of personnel whose employment has been terminated, who have been transferred, or whose accounts have been inactive for an extended period of time.

h. Making the final disposition (e.g., deletion) of the accounts and the information stored under those accounts.

i. Managing sessions and authentication and implementing account time-outs.

j. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.

k. Testing information resources to ensure security mechanisms are functioning properly.

l. Tracking hardware and software vulnerabilities.

m. Maintaining an accurate inventory of Postal Service information resources under their control.

n. Ensuring that audit and operational logs, as appropriate for the specific platform, are implemented, monitored, protected from unauthorized disclosure or modification, and are retained for the time period specified by Postal Service security policy.

o. Reviewing audit and operational logs and maintaining records of the reviews.

p. Identifying anomalies and possible internal and external attacks on Postal Service information resources.

q. Reporting information security incidents and anomalies to their manager and CyberSafe immediately upon detecting or receiving notice of a security incident.

r. Protecting information resources at risk during security incidents, assisting in the containment of security incidents as required, and taking action as directed by CyberSafe.

s. Participating in follow-up calls with CyberSafe and fixing issues identified following an incident.

t. Ensuring that virus protection software and signature files are updated and kept current for resources under their control.

u. Ensuring the availability of information resources by implementing backup and recovery procedures.

v. Ensuring the compliance with Postal Service information security policy and procedures.

w. Monitoring the implementation of network security mechanisms to ensure that they are functioning properly and are in compliance with established security policies.

x. Maintaining a record of all monitoring activities for information resources under their control.

y. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.

z. Resolving identified vulnerabilities.

2-2.~~3~~233 Database Administrators

Database administrators (DBAs) are responsible for the following:

a. Implementing appropriate database security based on the platform specific hardening standards for the information resources under their control.

b. Implementing information security policies and procedures for all database platforms and monitoring the implementation of database security mechanisms to ensure that they are functioning properly and are in compliance with established policies.

c. Applying approved patches and modifications, in accordance with policies and procedures established by the Postal Service.

d. Maintaining an accurate inventory of Postal Service information resources under their control.

e. Implementing appropriate database security administration and ensuring that log-on IDs are unique.

f. Setting up and managing accounts for systems under their control in accordance with policies and procedures established by the Postal Service.

g. Disabling accounts of personnel that have been terminated, transferred, or have accounts that have been inactive for an extended period of time.

h. Making the final disposition (e.g., deletion) of the accounts and the information stored under those accounts.

i. Managing sessions and authentication and implementing account time-outs.

j. Preventing residual data from exposure to unauthorized users as information resources are released or reallocated.

k. Testing database software to ensure that security mechanisms are functioning properly.

l. Tracking database software vulnerabilities, and deploying database security patches.

m. Ensuring database logs are turned on, logging appropriate information, protected from unauthorized disclosure or modification, and retained for the time period specified.

n. Reviewing database audit logs and maintaining records of log reviews.

o. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.

p. Ensuring the availability of databases by implementing database backup and recovery procedures.

q. Identifying anomalies and possible attacks on Postal Service information resources.

r. Reporting information security incidents and anomalies to their manager and CyberSafe immediately upon detecting or receiving notice of a security incident.

s. Protecting information resources at risk during security incidents, assisting in the containment of security incidents as required, and taking action as directed by CyberSafe.

t. Resolving identified vulnerabilities.

2-2.~~3334~~ All Personnel

All personnel, including employees, suppliers, consultants, contractors, business partners, customers who access non-publicly available Postal Service information resources (e.g., mainframes or the internal Postal Service network), and other authorized users of Postal Service information resources are responsible for the following:

a. Complying with applicable laws, regulations, and Postal Service information security policies, standards, and procedures.

b. Displaying proper identification while in any facility that provides access to Postal Service information resources.

c. Being aware of their physical surroundings, including weaknesses in physical security and the presence of any authorized or unauthorized visitor.

d. Protecting information resources, including workstations, portable devices, information, and media.

e. Always using their physical and technology electromechanical access control identification badge or device to gain entrance to a controlled area.

f. Ensuring no one tailgates into a controlled area on their badge.

g. Performing the security functions and duties associated with their job, including the safeguarding of their log-on IDs and passwords.

h. Changing their password immediately, if they suspect that the password has been compromised.

i. Prohibiting any use of their accounts, log-on IDs, passwords, personal information numbers (PINs), and tokens by another individual.

j. Taking immediate action to protect the information resources at risk upon discovering a security deficiency or violation.

k. Only using licensed and approved hardware and software.

l. Protecting intellectual property.

m. Complying with Postal Service remote access information security policies, including those for virtual private networks, modem access, dial-in access, secure telecommuting, and remote management and maintenance.

n. Complying with acceptable use policies.

o. Maintaining an accurate inventory of information resources for which they are responsible.

p. Protecting information resources against viruses and malicious code.

q. Calling the appropriate Help Desk for technical assistance in response to suspected virus incidents.

r. Immediately reporting to CyberSafe via telephone or email and, as appropriate, to their immediate supervisor, manager, or system administrator, any suspected security incidents, including security violations or suspicious actions, suspicion or occurrence of any fraudulent activity; unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information; and potentially dangerous activities or conditions.

s. Taking action, as directed by CyberSafe, to protect against information security incidents, to contain and eradicate them when they occur, and to recover from them.

t. Documenting all conversations and actions regarding the security incident and completing PS Form 1360, *Information Security Incident Report,* or an acceptable facsimile.

u. If an individual removes a portable electronic device from a Postal Service facility, he or she must do the following:

(1) If the device contains sensitive-enhanced or sensitive information, request approval in writing from his or her functional area vice president (data steward), CPO, and the VP IT Operations or their designees.

(2) Protect the device and the data it contains.

(3) Keep the device within sight, secured with a cable lock, or locked in a cabinet or closet.

(4) Do not check the device in baggage on an airplane, train, or any other public transportation.

(5) If an individual must leave the device in his or her vehicle, keep the device out of sight in a locked trunk. Never leave the device in a vehicle overnight.

(6) Use Postal Service-approved encrypted flash drive or encrypt sensitive-enhanced and sensitive data on the hard drive or other removable media using WinZip or Encryption File System (EFS).

v. Reporting any missing or stolen device or media immediately to his or her manager, CyberSafe via e-mail to *CyberSafe@usps.gov,* and to the local Inspection Service office. If the device has been stolen somewhere other than Postal Service premises, report the theft to the local police as well.

~~v.~~w. Complete all security training required by the Postal Service for their specific role.

3 Information Designation and Control

3-1 Policy

Postal Service information resources must be protected from time of collection to retirement, disposal, and destruction commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Postal Service's ability to conduct its mission.

All personnel must implement the protection requirements for information resources associated with information designation, categorization, and protection (including labeling, handling, controlling access and retention, protecting in transit and in storage, disposal, and destruction).

The following roles are vital to the protection of Postal Service Information:

a. The data owner is the executive with statutory and operational authority or specified information and responsibility for overseeing its generation, collection, processing, dissemination, disposal, and for the business results from using the information. The owner is responsible for ensuring that appropriate steps are taken to protect the information and for the implementation of policies, guidelines, and memorandums of understanding that define the appropriate use of the information.

b. The data steward is the manager with responsibility for providing business users with high-quality data that is easily accessible in a consistent manner. Data stewardship focuses on tactical coordination and implementation. Data stewards are responsible for carrying out data usage and security policies determined by the data owner or through enterprise data governance initiatives. Data stewards provide agreed-upon data definitions and formats and ensure that business users adhere to specified standards. They often collaborate with data architects; business intelligence developers; extraction, transformation, and load (ETL) designers; business data owners; and others to uphold data consistency and data quality metrics.

c. The data custodian is responsible for administrative and operational control over the information and for granting access to the information based on direction provided by the data steward.

Chapter 3 addresses the following:

a. Information designation and categorization.

b. Determination of the categorization of information resources.

c. Security requirements categories.

d. Protection of Postal Service information and media.

e. Protection of non-Postal Service information.

The Postal Service must develop data security policies using a set of data security standards, guidelines and requirements based on industry best practices that reflect levels of sensitivity further defined in this chapter according to privacy, access, retention, disposal, incident management, disaster recovery, and configuration management. Data or information designation, classification, and control is the process of sorting data or information into groups based on sensitivity and/or criticality.

In essence, a classification system contains all data at a particular level of criticality, or sensitivity. Classifications allow the organization to make rational decisions about the value of data of a certain type. The Postal Service will assign an appropriate degree of control for each type based on business value. The assignment creates layered groups of control at different levels of sensitivity and/or criticality.

The items in the group of highest priority are fully protected, while items of lesser value will still be given some protection appropriate to their relative status in the priority queue.

The term that is commonly used to describe the outcome of a classification process is "defense in depth." Classification levels are implemented hierarchically; each successive layer describes an increasingly rigorous degree of control, which is required to ensure integrity. Every level implements a well-defined set of rules that ensures that access is restricted only to those individuals who have been authorized. Establishing classification levels within an organization controls the resource allocation process efficiently for compliance. The classification definitions allow the Postal Service to make intelligent choices about how to protect three simple groupings of data rather than an uncounted number, or ad-hoc division of individual items. In conventional practice, these three groupings are labeled "unclassified" (any item of data that has not received a classification as defined by the USPIS as national security), "classified", and "classified under Executive Order 13526 or the Atomic Energy Act", as amended.

3-2 Information Designation and Categorization

Information at the Postal Service is designated and categorized based on the classification, sensitivity, and criticality of the information.

3-2.1 Potential Impact and Risk of Harm

All Postal Service personnel who have access to sensitive and sensitive enhanced information have a duty and responsibility to safeguard and protect the confidentiality and integrity of sensitive and sensitive-enhanced business and personal information against theft, unauthorized access, disclosure, along with manipulation or misuse of Postal Service information.

Such actions could result in substantial harm to the Postal Service brand, its business operations, financial operations and information systems, along with embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. Examples of harm include loss of control or misuse of information, damage to the trusted Postal Service brand, financial 3-2.4.1

loss, fiscal damage, exposure to possible law suits, and other negative impacts which adversely affect one or more individuals through fraud, manipulation or identity theft, or undermine the integrity of a system or program.

3-2.2 Designation Categories and Levels

Exhibit 3-2.2 defines classification, sensitivity, and criticality designation categories and levels.

Exhibit 3-2.2
Designation Categories and Levels

Designation Category	Description	Levels *(In decreasing order of necessity to protect the confidentiality, integrity, and availability of the information)*
Classification	Classification levels determine the need to protect the confidentiality and integrity of information.	Classified – Hardcopy or electronic information or material that has been designated as classified pursuant to executive order, statue, or regulation and requires protection against unauthorized disclosure for reasons of national security. Unclassified – Hardcopy or electronic information or materials that includes both sensitive but unclassified and non-sensitive which at a minimum must be safeguarded against tampering, destruction or loss.
Sensitivity	Sensitivity determines the need to protect the confidentiality and integrity of sensitive information.	Sensitive-Enhanced Unclassified Information (hereafter referred to as Sensitive-Enhanced) Sensitive Unclassified Information (hereafter referred to as Sensitive) Non-sensitive Unclassified Information (hereafter referred to as Non-sensitive)
Criticality	Criticality reflects the need for continuous availability of the information.	Critical (High) Critical (Moderate) Noncritical

3-2.3 Sensitivity and Criticality Category Independence

Sensitivity and criticality are independent designations. All Postal Service information must be evaluated to determine both sensitivity and criticality. Information with any sensitivity level may have any level of criticality level and vice versa.

3-2.4 Definitions of Classified, Sensitive, and Critical Information

3-2.4.1 Classified Information

Classified information is hardcopy or electronic information or material that has been designated as classified pursuant to executive order, statue, or regulation and requires protection against unauthorized disclosure for reasons of national security. National security reasons includes national defense, foreign relations of the United States, intelligence activities, atomic weapons and special nuclear material, crypto logic activities related to national security, command and control of military forces, integral components of weapon systems, or critical to direct fulfillment of military or 3-

2.4.2 intelligence missions. Classified designations include Confidential, Secret, and Top Secret. Categories of classified information include restricted data (RD), formerly restricted data (FRD), and national security information (NSI).

Note: Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

3-2.4.2 Sensitive-Enhanced Information

Sensitive-enhanced information is hardcopy or electronic information or material that is not designated as classified but that warrants or requires enhanced protection. Requirements to protect sensitive-enhanced information are derived from law, regulation, the law enforcement and judicial process, the payment card industry (PCI), and the Privacy Act. Types of sensitive-enhanced information include:

a. Law enforcement information and court-restricted information, including grand jury material, arrest records, and information about ongoing investigations.

b. PCI primary account number (PAN); i.e., full credit card number (16 characters).

c. Personally identifiable information (PII), i.e., information used to distinguish or trace an individual's identity such as name, Social Security number, driver license number, passport number, bank routing with account number, date with place of birth, mother's maiden name, biometric data, and any other information which is linked or linkable to an individual.

d. Information about individuals (e.g., employees, contractors, vendors, business partners, and customers) protected by law, including medical information and wire or money transfers.

e. Information related to the protection of Postal Service restricted financial information, trade secrets, proprietary information, and emergency preparedness.

f. Communications protected by legal privileges (e.g., attorney-client communications encompassing attorney opinions based on client supplied information) and documents constituting attorney work products (created in reasonable anticipation of litigation).

3-2.4.3 Sensitive Information

Sensitive information is hardcopy or electronic information or material that is not designated as classified or sensitive-enhanced but that warrants or requires protection. Requirements to protect sensitive information are derived from law, regulation, the Privacy Act, business needs, and the contracting process. Types of sensitive information include:

a. Private information about individuals (e.g., employees, contractors, vendors, business partners, and customers) including marital status, age, birth date, race, and buying habits.

b. Confidential business information that does not warrant sensitive-enhanced protection including trade secrets, proprietary information, financial information, contractor bid or proposal information, and source selection information.

c. Data susceptible to fraud including accounts payable, accounts receivable, payroll, and travel reimbursement.

d. Information illustrating or disclosing information resource protection vulnerabilities, or threats against persons, systems, operations, or facilities such as physical, technical or network/DMZ/enclave/ mainframe/server/workstation specifics including security settings, passwords, and audit logs.

3-2.4.4 Non-sensitive Information

Information that is not designated as classified, sensitive-enhanced, or sensitive information is by default designated as non-sensitive information. An example is publicly available information. Even though information is designated as non-sensitive information, it must still be protected (i.e., baseline requirements apply to all Postal Service information). Non-publicly available information must not be sent over the Internet unprotected (e.g., unencrypted).

3-2.4.5 Critical (High) Information

Information is designated as critical (high) information if its unavailability would have a catastrophic adverse impact on the following:

a. Customer or employee life, safety, or health.
b. Payment to suppliers or employees.
c. Revenue collection.
d. Movement of mail.
e. Communications.
f. Legal or regulatory.

3-2.4.6 Critical (Moderate) Information

Information is designated as critical (moderate) information if its unavailability would have a serious adverse impact on the following:

a. Customer or employee life, safety, or health.
b. Payment to suppliers or employees.
c. Revenue collection.
d. Movement of mail.
e. Communications.
f. Legal or regulatory.
g. Infrastructure services.

3-2.4.7 Noncritical Information

Information that is not designated as critical (high) or critical (moderate) is by default designated as noncritical.

3-3 Determination of the Categorization of Information Resources

3-3.1 Business Impact Assessment

Business Impact Assessment (BIA) is the process of identifying the consequences of current or proposed actions. The "impact" is the difference between what would happen with the action and what would happen without it. The Postal Service uses the following two types of impact assessments:

a. Internal.
b. External.

3-3.1.1 Internal Business Impact Assessment

The Internal Business Impact Assessment (BIA) is a process for determining the categorization of Postal Service information resources. A BIA must be completed for all information resources, whether the information resource is developed in house, outsourced or hosted in non-Postal Service facilities. The BIA must be updated periodically as required (every one or three years depending on its sensitivity designation), whenever a significant change is made to the information resource, or whenever the certification and accreditation (C&A) process is re-initiated.

The criteria for initiating a recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process,* 6-2.

Various stakeholders [e.g., management, operational personnel, and information systems security officers (ISSOs)] need to be involved in the BIA process. An information resource may process several information types. Each information type is subject to security categorization. The stakeholders must consider the consequences of unauthorized disclosure of sensitive-enhanced or sensitive information with respect to violations of federal policy and law. The impact of the violations will depend in part on the penalties associated with violation of the relevant statutes and policies. A privacy impact assessment (PIA) is included in the BIA.

The impact level for an information resource will normally be the highest impact level for the following security objectives associated with the information types:

a. Confidentiality — Preserving authorized restrictions on information access and disclosure.
b. Integrity — Guarding against improper information modification or destruction.
c. Availability — Ensuring timely and reliable access to information.

However in some cases, the security category for a system may be higher than any impact level for any information type processed by the system. Variations in sensitivity/criticality with respect to time may also need to be factored into the impact assessment process. Some information loses its sensitivity in time (e.g., a Postal Service rate increase becomes non-sensitive after it has been published). Some applications are particularly critical at

some point in time (e.g., the payroll application on the day for normal processing).

3-3.1.2 External Assessments

Security provisions are carried out by the Cloud Service Provider (CSP). Postal Service data is stored in a custom database schema designed by the provider. The Postal Service does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings. The CSP must ensure Postal Service data is protected from unauthorized access, use, disclosure, disruption, modification or destruction to ensure integrity, confidentiality, and availability. The CSP must comply with the current version of the Payment Card Industry (PCI) Data Security Standard (DSS) and the Information Supplement PCI/DSS Cloud Computing Guidelines. All cloud solutions must demonstrate the ability to meet the Postal Service security requirements.

The Postal Service requires external providers handling Postal data and/or information resources or operating systems to meet the same security standards and requirements as internal users. The Postal Service must ensure that privacy and security controls and safeguards are implemented with maximum operational functionality to meet baseline privacy and security requirements and employ risk mitigation strategies and assessments.

3-3.1.3 Cloud Computing Impact Assessment.

The Consolidated Cloud Computing Impact Assessment (CCIA) is part of the Cloud Computing Certification and Accreditation security evaluation and assessment process. It is used to gather initial information on a cloud solution operating on a FedRAMP certified infrastructure. Refer to Handbook AS-805H, *Cloud Computing,* which includes responsibilities and instructions for completing the questionnaire. In most cases, the Information Systems Security Officer (ISSO) along with the Information systems security representatives (ISSR) will complete the questionnaire section of this document.

The purpose of the Consolidated Cloud Computing Impact Assessment is to identify the appropriate privacy and security requirements to protect Postal Service information resources, organization, and personnel.

The Consolidated CCIA ensures that cloud systems processing or storing customer or personnel information, or technologies that can be used for monitoring purposes adhere to Postal Service privacy requirements. Privacy requirements are based on applicable privacy laws, such as the Privacy Act, as well as privacy policies that the Postal Service has adopted. Compliance with privacy requirements is addressed in Section 4 of the Questionnaire.

3-3.2 Aggregation

Some information may have little or no sensitivity in isolation but may have high sensitivity in aggregate. In some cases, aggregation of large quantities of a single information type can reveal patterns and/or plans, or facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous information types

can have similar effects. In general, the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of a bank account number with the identity of an individual and/or institution).

The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system categorization may need to be adjusted to a higher level than would be indicated by the impact associated with any individual information type.

3-3.3 System Functionality

Compromise of some information types may have low impact in the context of a system's primary function but may have much more significance when viewed in the context of the potential impact of compromising:

a. Other systems to which the system in question is connected, or

b. Other systems which are dependent on that system's information.

Access control information for a system that processes only low-impact information might initially be thought to have only low-impact attributes. However, if access to that system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered.

Similarly, some information may, in general, have low-sensitivity or criticality attributes. However, that information may be used by other systems to enable sensitive-enhanced, sensitive, or critical functions. Loss of data integrity, availability, temporal context, or other context can have severe consequences.

3-3.4 Critical National Infrastructure

Where the mission served by an information system, or the information that the system processes affects the security of the critical national infrastructure, the loss of confidentiality, integrity, or availability could result in a higher designation.

3-3.5 Approving Information Resource Classification and Categories of Information Processed

The determination of the sensitivity for each information resource and the categories of information processed must be approved by the chief privacy officer (CPO) or his or her designee through the BIA. The determination of the criticality for each information resource must be approved by the postmaster general and his senior executives. This process is facilitated by the manager of Business Continuance Management or his or her designee.

3-3.6 Recording Information Resource Classification and Categories of Information Processed

The sensitivity and criticality for each information resource and the categories of information processed must be documented in the Enterprise Information Repository (EIR) and in the information security plan.

3-4 Security Requirement Categories

The Postal Service uses several categories of security requirements to protect information resources (see Exhibit 3-4).

A security requirement is a type or level of protection that must be implemented to secure an information resource. A control consists of safeguards designed to respond to a security requirement. A control may satisfy more than one requirement, or several controls may be needed to satisfy a security requirement depending on the sensitivity and criticality of the information resource and its operating environment. If a requirement cannot be addressed, compensating controls can be implemented to mitigate the risk.

Exhibit 3-4
Security Requirement Categories

Security Requirement Category	Control(s)
Baseline	All information resources must implement controls sufficient to satisfy the baseline security requirements. Baseline security requirements have been established to protect the Postal Service computing environment and infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction.
Sensitive-Enhanced, Sensitive, PCI, Law Enforcement, Critical (High), and Critical (Moderate)	Additional security is needed to adequately protect sensitive-enhanced, sensitive, and critical information resources. These requirements are based on the following: ■ Sensitivity and criticality of the information resource. ■ Federal legislation [e.g., the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act. ■ Federal regulations (e.g., requirements for cryptographic modules). ■ Federal directives (e.g., personal identity verification and critical infrastructure). ■ Industry requirements (e.g., all developers and service providers of PCI in-scope applications must comply with the current PCI Data Security Standard).
Conditional	Requirements requested by the executive VP and CIO; VP IT Solutions; Director IT Operations; manager, CISO; or the functional VP or requirements based on specific criteria such as the development and operating environment.
Recommended	ISSOs may recommend additional security requirements during the BIA process to better protect the information resource against threats and vulnerabilities. Recommended security requirements are based on generally accepted industry practices. The executive sponsor assumes the risks associated with not implementing the recommended security requirements.

3-5 Protection of Postal Service Information and Media

All Postal Service information must be properly handled and controlled. While the focus of information security is on protecting sensitive-enhanced and sensitive information which is driven by government regulation and industry standards, the Postal Service must also protect non-publicly available

information. Non-publicly available information must be protected by the same controls as sensitive and sensitive-enhanced information, e.g., encryption. If there are questions concerning the appropriate security controls to implement, consult with CISO.

The level of protection must be based on the information's sensitivity and criticality, e.g., full and partial social security numbers must only be used for tax purposes and must not be used for identification purposes and must not be printed on reports.

Labeling, retention, storage, encryption, release, and destruction of information must comply with the Postal Service policies specified in this section and in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management.*

3-5.1 Labeling of Information, Media, and Devices

3-5.1.1 Electronic Media and Hardcopy Output

The Postal Service processes, stores, and transmits many types of sensitive information. Appropriately labeling the media helps ensure that all recipients of the material are aware that the information requires protection.

Note: If information with different levels of sensitivity is combined, the total package must be protected at the sensitivity level of the information that has the greatest sensitivity.

The following definitions apply within this section:

a. Hardcopy Material – Printed material, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

b. Label – A RESTRICTED label may be internal or external as follows:

(1) Internal Label – A RESTRICTED marking within the confines of the medium.

(2) External Label – A RESTRICTED marking on the outside of the medium, or a cover.

c. Storage Media – Includes but is not limited to magnetic storage media such as hard disk drives and diskettes; optical storage media such as CDs and DVDs; solid-state storage media, including USB drives; and hardcopy materials, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

3-5.1.2 Applications Processing

On applications processing sensitive-enhanced or sensitive information, the following statement must be prominently displayed on the login/password screen or the welcome screen: "Information within this application is designated sensitive-enhanced (or sensitive) and should be properly protected from unauthorized access or disclosure." Additionally, the "Print Screen" function can also result in hardcopy that must be legibly and durably labeled as "RESTRICTED INFORMATION."

3-5.1.3 Devices

All in-scope PCI devices must be labeled with owner, contact information, and purpose.

3-5.2 Controlling Access to Information

Access to information in hardcopy and digital form must be restricted to authorized personnel as follows:

a. To prevent unauthorized access to hardcopy and electronic media, one of the following controls must be employed:

(1) A locked desk or file cabinet.

(2) A room with a key, combination, or electronic lock.

(3) An approved media storage area or an area behind a guard.

b. To prevent unauthorized access to electronic files and databases, access controls must be employed. Access attempts granted and refused are subject to audit.

c. Sensitive-enhanced and sensitive information must be protected from unauthorized access and disclosure. Access must be restricted to authorized personnel with a need to know. The functional system coordinator (FSC), as an agent of the executive sponsor (data steward), controls access based on role and level of access requested.

d. Metadata (i.e., data describing the structure, content, and context of electronic information) must also be protected from unauthorized access and disclosure.

e. Critical information must be protected from unauthorized access and destruction.

f. The PCI primary account number (PAN) must be masked when displayed and/or printed (the first six or the last four digits are the maximum digits that may be displayed or printed), such that only personnel with a legitimate business need for the information to perform their job (e.g., to process or manage transactions or chargebacks) can see the full PAN.

g. PANs must be de-identified or removed from tables, files, removable media, and audit logs.

h. All personnel with authorization to handle and/or view cardholder data must follow the PCI Data Security Standard (DSS) requirements to protect this type of sensitive-enhanced data.

3-5.3 Retention and Storage of Information

The retention and storage of information must be controlled as follows:

a. All Postal Service information must be retained in accordance with legal retention requirements established by law (e.g., legal holds), and also with operational retention requirements established by the business owner with concurrence by the Postal Service Privacy and Records Office, Legal, and the Inspection Service (see Handbook AS-353).

b. When the retention period or legal hold has expired, sensitive-enhanced, sensitive, and critical information must be properly destroyed as described in *Disposal and Destruction of Information and Media*. The process of removing expired information can be automated or manual.

c. Sensitive-enhanced, sensitive, and critical information should be stored in a controlled area or a locked cabinet in accordance with established Postal Service policies and procedures.

d. PII must not be stored or accessed on devices that are located outside of the United States.

e. Sensitive-enhanced information must not be processed or stored in a public cloud.

f. PCI and law enforcement information must be stored in an enclave.

g. Under no circumstances should non-publicly available information be stored on a public Web site.

h. Non-publicly available Postal Service information must be isolated and stored separately from non-Postal Service information (e.g., business partner and vendor information) unless required by law or regulation. Non-publicly available Postal Service information and non-Postal Service information must be stored separately at Postal Service facilities, non-Postal Service facilities, or at backup sites unless required by law or regulation.

i. Payment cardholder information must not be copied or stored on local hard drives or removable electronic media as the result of accessing such data via remote access technologies.

j. Payment cardholder electronic media must be inventoried and the inventory reconciled semiannually.

k. Cardholder data storage must be kept to a minimum and retention time must be limited.

l. The following PCI authentication data must not be stored (e.g., log files, history files, trace files, database contents, etc.) after completing the payment transaction under any circumstance:

   (1) The full contents of any track from the magnetic stripe on the back of the card or contained in a chip on the card.

   (2) The three-digit or four-digit card-validation code printed on the front of the card or the signature panel on the back of the card.

   (3) PINs or the encrypted PIN blocks.

m. Temporary storage of PCI authentication data must be deleted in a manner that makes the data unrecoverable.

n. PANs must be rendered unreadable anywhere they are stored by one way hash, truncation, indexed tokens, or strong cryptography.

o. Retention of payment card data is defined in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management.* A quarterly automatic or manual process must be implemented for identifying and securely deleting cardholder data that exceeds the defined retention requirement.

p. Program-level and project-level TSLC artifacts and compliance records must be kept as long as the program/project is active and must be purged 27 months after the program/project is retired.

3-5.4 Encryption of Information

Examples of conditions under which Postal Service information must be encrypted include, but are not limited to, the following:

a. Sensitive-enhanced and sensitive information in transit across networks.

b. Sensitive-enhanced and sensitive data in transit between [1] an application or batch server and a database server and [2] between workstations and a database server.

c. Sensitive-enhanced and sensitive information at rest including information stored or archived on removable devices or media including disks, diskettes, CDs, and USB storage devices.

d. Sensitive-enhanced and sensitive information that is stored off Postal Service premises.

e. PCI information (encrypted throughout the life cycle).

f. Non-publicly available electronic information in transit or stored off Postal Service premises.

g. For portable Public Key Infrastructure (PKI) backup media, see 9-7.1 for encryption compliance methods.

3-5.5 Mandatory Requirements and Procedures for Authorized Removal of Postal Service Non-Publicly Available Information from Postal Service or Business Partner Premises

3-5.5.1 Definition of Non-Publicly Available Information

Non-publicly available information includes

a. Sensitive-enhanced information (see 3-2.4.2).

b. Sensitive information (see 3-2.4.3).

c. Non-sensitive information that the Postal Service does not want to disclose at this time.

3-5.5.2 Definition of Removal from Postal Service or Business Partner Premises

Removal from Postal Service or business partner premises includes:

a. Removal by remote access, with (or without) downloading or forwarding.

b. Removal by directed transmission through third-party services.

c. Removal from premises of digital copies stored on portable computers or any type of media.

d. Removal from premises in hard-copy format.

e. Printing off premises.

f. Sending a facsimile off premises.

g. Contractor shredding or destruction off premises.

h. Information directly collected on behalf of the Postal Service by a Business Partner or third-party service provider, e.g., an application that is externally hosted with all data collected by the Business Partner.

i. Information sent to a Business Partner as part of a Service-Based Contract.

3-5.5.3 Mandatory Requirements and Procedures for Authorized Removal Of Electronic and Hard-copy Information

The removal authorization must be approved in ~~eAccessARISe~~Access/ARIS and a list of all personnel with removal authorization must be available on request.

Before removal, the following approvals are required:

(1) Functional VP or designee (data steward).

(2) CPO or designee.

(3) CIO or CIO's designee (data custodian).

a. All physical functions (e.g., pickup, acceptance, reception, transfer, or delivery) related to removal of non-publicly available information must be conducted by authorized personnel whose identity is verified by a check of the Postal Service badge.

b. Two-factor authentication is required for electronic access or removal.

c. All non-publicly available electronic information that is accessed, processed, or stored at non-Postal Service sites must be encrypted and processed on either (1) Postal Service-owned hardware and software (2) on business-partner-owned hardware and software that meets all of the following requirements:

(1) Offsite Hosting Letter approved by:

(a) Functional VP or designee.

(b) Manager, CISO or designee.

(c) CIO or designee.

(2) Written stipulation that it meets Postal Service server hardening and malicious code protection standards.

(3) Written consent to unannounced audits.

e. All ACE-supported infrastructure components in use must be connected at least weekly over a secure link to the Postal Service intranet to receive appropriate security patches and virus recognition patterns.

Non-ACE-supported components must be appropriately patched and have the latest virus recognitions patterns installed.

f. All non-publicly available electronic information must be encrypted as follows:

(1) All types of storage off Postal Service premises including mobile devices such as laptops and portable media.

(2) All transmissions.

g. PCI cardholder information must not be stored off Postal Service premises on any device or media, including: hard drives, USB thumb drives, disks, PDAs, cell phones, or laptops.

h. All Postal Service (and/or business-partner-owned) electronic devices and electronic media (including backups) containing non-publicly available information and all hard copies must be effectively secured against theft and/or unauthorized access (e.g., controlled areas, safes, locked cabinets).

i. All removals of non-publicly available information must be concurrently documented to ensure accountability in the life cycle management of that information. All such data and all copies must be inventoried annually and formally tracked (e.g., logbook, tape management system) from creation to destruction. This inventory and tracking log must be updated with each transfer/removal and be available for audit.

3-5.6 Release of Information

The release of information must be accomplished in accordance with Postal Service policies and procedures (see Handbook AS-353).

Sensitive-enhanced and sensitive information must be protected from unauthorized disclosure, whether formally or informally through conversations, e-mail, voice, printing, facsimile, shredding, destruction, and observed workstation screens or whiteboards.

3-5.6.1 Releasing Information on Factory-Fresh or Degaussed Media

Before releasing information on electronic media outside the Postal Service, the information must be copied onto factory-fresh media (never used) or onto media that was appropriately degaussed to prevent inadvertent release of sensitive-enhanced and sensitive information.

3-5.6.2 Precautions Prior to Maintenance

To prevent inadvertent disclosure of sensitive-enhanced and sensitive information, all hardware and electronic media being released for maintenance outside of Postal Service facilities must, prior to release, undergo data eradication according to approved Postal Service procedures. If electronic media containing sensitive-enhanced and sensitive information is released to a contractor or vendor for maintenance, the Postal Service must have in place a legally binding contract regarding the secure handling and storage of the data or media.

3-5.7 Handling Biohazard Contaminated Information Resources

3-5.7.1 Sensitive-Enhanced and Sensitive Information

Any personnel handling biohazard contaminated Postal Service information resources must follow the standards set forth by the Inspection Service for handling contaminated devices. If the contaminated information resource contains sensitive-enhanced and sensitive information, the Inspection Service must be notified regarding the type of device, the classification of data it contains (i.e., sensitive-enhanced or sensitive), and the Postal Service

manager responsible for the device. Disposition of the contaminated information resource must be recorded, including who took possession of the device and the disposition expected for the resource.

3-5.7.2 Data Eradication on Contaminated Information Resources

Any Postal Service hardware or electronic media being released outside of Postal Service facilities must, prior to release, undergo data eradication, if possible, according to approved Postal Service procedures. Eradication procedures may include the ability to eradicate data through remote management of the information resource. If data eradication is not possible, the Inspection Service must be advised and notification must be made to all persons involved in the chain of possession of their responsibility for nondisclosure of the information contained in the device. It is strongly recommended that a memorandum of nondisclosure be signed by all personnel involved in the chain of possession of the contaminated information resource.

3-5.7.3 Reporting of Contaminated Information Resources

The Postal Service manager responsible for the contaminated device must complete PS Form 1360, *Information Systems Security Incident Report,* to ensure appropriate security management notification of the status and disposition of the information resource.

3-5.8 Disposal and Destruction of Information and Media

3-5.8.1 Electronic Hardware and Media

To prevent inadvertent disclosure of sensitive-enhanced and sensitive information, all electronic hardware and media must, prior to being disposed of, undergo data eradication according to approved Postal Service procedures. Unacceptable practices of erasure include a high-level file erase or high-level formatting that only removes the address location of the file. Acceptable methods of complete erasure include the following:

a. Zero-bit formatting
b. Degaussing
c. Physical destruction
~~c.~~d. Crypto Erasure or Crypto Shredding

The results from zero-bit formatting and degaussing must be periodically tested to verify complete erasure.

Crypto Erasure or Crypto Shredding must follow validated processes to ensure that cryptographic keys are protected from inadvertent deletion as well as ensure that keys are deleted when the storage is to be erased.

Disposal contractors must have appropriate personnel clearances, physical security of the facility, and procedures to store and handle the equipment and media (that may contain sensitive-enhanced or sensitive information) before and during disposal. Disposal contractors must be certified by the National Association of Information Destruction.

For locations associated with a District Office, computing equipment no longer needed for current operations must be sent to the District Office for disposal

through the USPS MDC Topeka in Topeka, Kansas (Address: 7215 S.W. Topeka Blvd., Bldg. 7, Topeka, KS 66624-9998). For locations not associated with a District Office, computing equipment no longer needed for current operations must be sent directly to the USPS MDC Topeka.

Hardware device disposal must be recorded in a Postal Service asset management system by the appropriate IT support organization.

3-5.8.2 Data Residue

As resources are allocated to data objects or released from those data objects (i.e., object reuse), information resources must have the capability to ensure that no accessible data is exposed to unauthorized users. Information resources must:

a. Have the capability to overwrite memory and storage that renders the information unrecoverable to prevent disclosure of sensitive-enhanced and sensitive information.

b. Restrict the capability to overwrite memory and storage to an authorized user.

c. Ensure that any previous information content of a resource is made unavailable upon the re-allocation of the resource for usage.

d. Ensure memory and storage allocated to processing sensitive-enhanced and sensitive information, including PCI transactions and authorization data is cleared before reallocation.

3-5.8.3 Non-electronic Information

Non-electronic information designated as sensitive-enhanced or sensitive must be destroyed by cross-cut shredding, pulping, or burning when no longer needed if the information is not subject to a legal hold and the retention period has expired.

Containers holding non-electronic information to be shredded must be constructed with suitable materials and a lock to prevent unauthorized access (e.g., a container similar to a mail collection box painted red).

3-5.9 Protection of Postal Service Information during International Travel

3-5.9.1 General Security Requirements While Traveling Outside of the United States

The transfer of files via portable storage devices, compact disks, and other file-sharing technology, exposes Postal Service systems to the possibility that information may be intentionally or inadvertently obtained by non-Postal Service personnel, or that malicious software may be transferred to Postal Service systems. Therefore, use of portable media and access to networks should be limited to only what is necessary for successful fulfillment of the international Postal Service mission and must be encrypted.

Any loss of devices suspected compromise or unusual computer activity ~~should~~ must be reported to USPS CyberSafe *CyberSafe@usps.gov* before the computer is again connected to the Postal Service network.

Postal Service computers and mobile devices must not be taken outside of the United States on personal travel. Mobile devices are defined in 10-2.4 and 10-2.5.

Note: The Department of Homeland Security (DHS) may search, copy, and/or retain laptops, PDAs, USB devices, and other digital devices without cause at U.S. borders.

3-5.9.2 Substitution of Temporary Computer Equipment and Communication Devices

For some high-risk international destinations, users on official Postal Service business will be prohibited from traveling with their standard issue computers and mobile computing devices. In these instances, temporary equipment will be provided for the international mission by IT and the device will be wiped upon return.

3-5.10 Inclusion of Protection Requirements in Contracts

3-5.10.1 All Business Partners and Suppliers

Information security and privacy requirements must be included in all contracts involving Postal Service information.

The business partner or supplier must be compliant, at its own expense, with current federal legislation, federal regulations, federal directives, and industry requirements. To be enforceable, these requirements must be included in the contract. The Postal Service organization developing the requirements must either include them in the Statement of Work or work with the Contracting Officer to ensure such requirements are in the contract. The Postal Service or its designee may conduct audits of the business partner or supplier system and associated processes to assure compliance. In the event of noncompliance or a data breach, the business partner or supplier accepts full responsibility for all fines, lawsuits, and investigation and mitigation costs incurred by Postal Service resulting from such events.

3-5.10.2 Payment-Card Business Partners and Suppliers

Payment-card business partners and vendors must be compliant, at their own expense, with the Payment Card Industry (PCI) Data Security Standard (DSS), as amended or updated by the PCI Security Standards Council, and applicable to the Vendor Merchant or Service Provider Level as defined by the Visa Cardholder Information Security Program (CISP). The business partner or vendor is responsible for ensuring that its system performs each payment transaction in compliance with PCI-DSS requirements.

The Postal Service or its designee may conduct audits of the business partner or supplier payment systems and associated processes to assure PCI-DSS compliance. In the event of noncompliance or a data breach of the payment system or associated processes, the business partner or supplier accepts full responsibility for all fines, lawsuits, and investigation and mitigation costs incurred by the Postal Service resulting from such events. The business partner or supplier must accept these conditions in writing and provide a Letter of Attestation annually acknowledging their responsibility for the security of payment card data stored, processed, or transmitted on behalf of the Postal Service.

3-5.11 Additional PCI Requirements

PCI applications and cardholder information must reside on a restricted network segment or enclave on Postal Service premises. Cardholder information must not be stored off Postal Service premises on any device or media including hard drives, USB thumb drives, disks, diskettes, PDAs, smart phones, tablets, or laptops. ~~All PANs sent via mail or any other remote access technology must be encrypted with the Postal-approved encryption solution.~~ Non-USPIS personnel may not send customer cardholder data (other than the first six and last four digits) via any electronic communication (including, but not limited to, email) for any reason, regardless of whether a USPS-approved encryption solution is utilized.

All PCI PANs must reside in a PCI approved enclave. All PCI PANs discovered outside the PCI enclave by the Data Loss Protection (DLP) program will be handled as follows:

a. The file will be moved to the DLP enclave and encrypted.
b. A marker file will be put in its place.
c. The owner will be notified when an owner can be determined.
d. The owner is responsible for remediation.

On the request of the OIG for forensics or the Privacy Office for notification of the cardholder or the card provider, the file will be stored encrypted in the DLP enclave until such time as the analysis or notification process is completed. At which time the file will be deleted.

3-5.12 Additional PII Requirements

All Social Security Numbers discovered on Postal Service information resources that are not encrypted by the Postal-approved encryption solution will be handled as follows:

a. The file will be moved to the DPL enclave and encrypted.
b. A marker file will be put in its place.
c. The owner will be notified when an owner can be determined.
d. The owner is responsible for remediation.

On the request of the OIG for forensics or the Privacy Office for notification of the individual, the file will be stored encrypted in the DLP enclave until the analysis or notification process is complete. At which time the file will be deleted.

IT must use approved encryption methods that can be discovered by security DLP tools.

3-5.13 Protection of Financial information

Applications that maintain inventories (e.g., supplies, merchandise, money orders, stamps, equipment) or financial information (e.g., accounts payable, accounts receivable) must implement appropriate controls to protect the integrity of the inventory/financial information and the application processes and to ensure individuals with access do not enrich themselves at the expense of the Postal Service. Possible controls that must be considered are input validation, separation of duties, audit logging, data retention, analysis of

recipient addresses, check overprinting, control of check stock, and oversight of the printing and distribution process.

3-6 Protection of Non-Postal Service Information

3-6.1 Third-Party Information

Any information that does not belong to the Postal Service must be protected in accordance with legal requirements or contractual agreements with a third party except that when such requirements do not meet security standards for comparable Postal Service information, the Postal Service must meet or exceed its own standards.

3-6.2 National Security Classified Information

Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

3-7 Cyber Threat Information

Threat is any circumstance or event (human, physical, or environmental) with the potential to cause harm to an information resource in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting a vulnerability.

Cyber threats may include, but are not limited to, viruses, malware, Trojans, exploits, phishing attempts, and insider threats.

The objective of sharing cyber threat information is to support the overall CISO strategy and all information-sharing agreements, which must be approved by CISO leadership. The agreements must be coordinated with CISO units with a role in the collection, processing, storage, and protection of threat information.

An insider threat is a malicious or unintentional threat to an organization caused by the actions of a current or former employee, contractor, or business partner. Insider threats result from personnel exceeding or misusing their organizational access in a manner that affects the confidentiality, integrity, availability, or physical welfare of an organization's information, information systems, or workforce.

The Postal Service Insider Threat Program (InTP) works closely with the United States Postal Inspection Service (USPIS) and USPS Office of the Inspector General (OIG) to prevent, detect, and escalate instances of insider threat activity.

All threat information sharing must be managed within a Threat Intelligence Platform (TIP). The threat information-sharing process includes engaging in ongoing communication with partners, consuming security alerts and indicators, organizing and storing information, and producing and publishing information for sharing with partners.

Threat information sharing must comply with Postal Service legal restrictions on the type of information that may be shared, including the requirement that shared threat information must not be attributable to the Postal Service.

Information types, such as Personally Identifiable Information (PII), classified information, and Postal Service proprietary information, may not be shared and must be protected. Adequate security and privacy controls must be implemented to protect this information from unauthorized disclosure or modification.

4 Security Risk Management

4-1 Policy

Risk assessments are required for all information resources, whether developed and operated in house or by business partners to ensure cost effective protection of information, applications, information resources, and the continuity of business operations. Site security reviews are also required for all facilities that house sensitive-enhanced, sensitive, or critical information resources, regardless of where they are located. Based on the results of risk assessments and site security reviews, managers must develop (or acquire) and implement security measures to handle unexpected events, avoid unacceptable losses, and minimize the effect of emergencies on business operations. Chapter 4 addresses the following:

a. Types of risk management.

b. Information resource risk management.

c. Independent risk management.

d. Site risk management.

All information resource risk management documentation must be treated as "restricted information" delivered to and retained by the executive sponsor with a copy to the Corporate Information Security Office to ensure all risk mitigation decisions are consolidated and appropriately made for like risks across Postal Service.

4-2 Types of Risk Management

The Postal Service implements the following three types of risk management:

a. Information resource risk management.

b. Independent risk management.

c. Site risk management.

4-3 Information Resource Risk Management

A risk assessment must be completed for all information resources. The risk assessment must address the following areas:

a. Identify the assets at risk and their value to the organization.

b. Identify the threats.

c. Identify the weaknesses and vulnerabilities.

d. Evaluate threats and vulnerabilities to determine the risks that threaten loss of value.

e. Identify possible safeguards (e.g., controls and countermeasures).

f. Analyze the costs and benefits of the safeguards in reducing the risks.

g. Complete the information resource risk assessment report.

The risk assessment must be completed in conjunction with system development. Additional risks may be identified in each of the life-cycle phases as development progresses through requirements definition, design, coding, testing, and production. The risks must be re-assessed and the risk assessment report updated as follows:

a. Every year for a payment card industry information resource.

b. After a significant audit finding.

c. Whenever the information resource experiences significant enhancement or modification, including changes to the infrastructure, operating system, or hardware platform.

d. After an information security incident that violates an explicit or implied security policy and compromises the integrity, availability, or confidentiality of an information resource.

e. Every 2 years for sensitive-enhance, sensitive, critical high and moderate, and externally facing information resources as part of the recertification process unless an earlier re-assessment is warranted.

f. Every 3 years for non-sensitive and noncritical information resources as part of the recertification process unless an earlier re-assessment is warranted.

Risks categorized as high or medium must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures. The risk mitigation process consists of the following:

a. Selecting the appropriate safeguards (or countermeasures) that will reduce exposure to the risk.

b. Assigning a priority ranking to the implementation of the safeguards.

c. Assigning financial and technical responsibility for implementing the safeguards.

d. Implementing and documenting the safeguards.

e. Maintaining the continued effectiveness of the mitigation strategy by reassessing the threats, vulnerabilities, effectiveness of the safeguards, and the residual risk.

If the level of residual risk is not acceptable, then further safeguards and security controls should be implemented to reduce exposure to acceptable levels. The vice president of the functional business area is responsible for accepting (and the vice president, Information Technology Solutions is

responsible for acknowledging), in writing, the residual risks inherent with using that information resource or initiating steps to further mitigate the residual risk.

All information resource risk management documentation must be treated as "restricted information" delivered to and retained by the executive sponsor and a copy sent to the Corporate Information Security Office.

4-4 Independent Risk Management

An independent information risk assessment may be required during the business impact assessment process. Independent risk assessments are conducted by organizations that are separate and distinct from those responsible for the development and operation of the information resources. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for the criteria for conducting an independent risk assessment.)

4-5 Site Risk Management

A site security review must be performed for each site hosting sensitive-enhanced, sensitive, or critical information resources and may be required for business partner and vendor sites requesting connectivity to the Postal Service intranet to:

a. Identify the location of the facility and structure-specific strengths and weaknesses.

b. Identify the sensitive-enhanced, sensitive, and critical information resources hosted by that facility.

c. Identify the threat events that could occur, including physical threats (e.g., power failure, fire, building collapse, water damage from plumbing failure and roof leak); environmental threats (e.g., earthquake, flooding, tornadoes, lightning, and sink hole); and human threats (e.g., union lockouts, riot, disgruntled employee or customer, and armed theft).

d. Evaluate threats and vulnerabilities to determine the frequency and amount of harm that could possibly occur as a result of a physical, environmental, or human event.

e. Identify possible additional administrative, technical, and physical security safeguards.

f. Analyze the costs and benefits of the safeguards in reducing the risks.

A site security review is conducted at the following times:

a. Before a new site becomes operational.

b. After significant changes at the site, including significant changes in information resources located there.

c. Every 3 years, unless an earlier site security review is warranted.

Risks categorized as high must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures. The risk mitigation process consists of the following:

a. Selecting the appropriate safeguards (or countermeasures) that will reduce exposure to the risk.

b. Assigning a priority ranking to the implementation of the safeguards.

c. Assigning financial and technical responsibility for implementing the safeguards.

d. Implementing and documenting the safeguards.

e. Maintaining the continued effectiveness of the mitigation strategy by reassessing the threats, vulnerabilities, effectiveness of the safeguards, and the residual risk.

If the level of residual risk is not acceptable, then further safeguards and security controls should be implemented to reduce exposure to acceptable levels. The installation head is responsible for acknowledging and accepting the residual site risk.

The site security review will be performed by the manager CISO and the Chief Inspector or their designees. All site risk management documentation must be treated as "restricted information" and delivered to and retained by the Inspection Service and the appropriate installation head.

4-6 Risk-Based Information Security Framework

The risk-based information security framework [1] allows traceability from the highest-level strategic goals and objectives of the Postal Service, through specific mission/business protection needs, down to specific information security solutions and [2] incorporates information security requirements from legislation, directives, policies, regulations, standards, and guidance.

A risk-based strategy gives vice presidents of functional business areas, executive sponsors, and Business Relationship Management portfolio managers the opportunity to make informed risk-based decisions in dynamic operating environments—decisions based on trade-offs between fulfilling business functions and managing the many types and sources of risk that must be considered. Information security risks must be aligned with business risks to accurately gauge the effectiveness of information security controls.

The following key elements are required to effectively manage information security risks for the Postal Service:

- Assignment of risk management responsibilities to vice presidents of functional business areas, executive sponsors, and Business Relationship Management portfolio managers.

- Recognition and acceptance of the information security risks to Postal Service information resources, individuals, and other organizations (e.g., business partners, vendors, customers) arising from the operation and use of information systems.
- Establishing the tolerance for risk and communicating the risk tolerance throughout the Postal Service, including guidance on how risk tolerance impacts ongoing decision-making activities and the overall security stance of the Postal Service, not just to a specific information resource, process, or organization.
- Accountability by vice presidents of functional business areas, executive sponsors, and Business Relationship Management portfolio managers for their risk management decisions.

5 Acceptable Use

5-1 Policy

Postal Service information resources must be used in an approved, ethical, and lawful manner to avoid loss or damage to Postal Service operations, image, or financial interests and are used to comply with official policies and procedures on acceptable use. Personnel must contact the manager, Corporate Information Security Office, prior to engaging in any activities not explicitly covered by the following policies:

a. Personal use of government office equipment including information technology.

b. Electronic mail and messaging.

c. Internet.

d. Prohibited uses of information resources.

e. Protection of sensitive personal and Postal Service information.

All Postal systems (on premise, hosted, cloud) must display or provide a link to notify users of the Postal Service terms of use and privacy notice.

5-2 Personal Use of Government Office Equipment Including Information Technology

Management at each Postal Service facility may permit employees to make limited personal use of Postal Service office equipment, including information technology equipment, provided such use does not reduce or otherwise adversely affect the employee's productivity during work hours, does not interfere with the mission or operations of the Postal Service, and does not violate the Standards of Ethical Conduct.

The office equipment governed by this policy includes, but is not limited to, personal computers; personal digital assistants (including Blackberries); peripherals, such as printers and modems; computer software (including Web browsers); telephones; cell phones; smart phones; tablets; smart watches; facsimile machines; photocopiers; scanners; label writers; consumable office products; office supplies; removable media; library resources; Internet connectivity; remote-access technologies (e.g., VPN);

and e-mail. Use of Postal Service information resources constitutes permission to monitor that use.

Limited personal use of Postal Service office equipment, including information technology, means occasional use that meets the following criteria:

a. Is of limited duration, length, or size, and does not interfere with employees' official duties or the transaction of official Postal Service business.

b. Results in only minimal, if any, additional expense to the Postal Service or minimal wear and tear on Postal Service office equipment; uses a small amount of data storage; has only a small-to-moderate transmission impact; or requires only small amounts of consumable office products (e.g., ink, paper, toner, and computer memory).

Some examples of limited personal use are:

a. Making a few photocopies.

b. Make occasional, brief telephone calls that result in little or no cost.

~~c.~~ Sending an occasional facsimile of a few pages.

~~d.~~c. Sending a brief personal email message ~~is defined as an email~~ that contains only text (no urls, files, or images attached).

~~e.~~d. Doing a brief Internet search.

Limited personal use of Postal Service office equipment, including information technology, must not:

a. Reduce employee productivity or interfere with official Postal Service business (e.g., congest, delay, or disrupt any Postal Service system or equipment).

b. Be for the purpose of maintaining or promoting a personal or private business.

c. Be for the purpose of posting unauthorized commercial or advertising materials.

d. Be for any illegal purpose, including, but not limited to, gaining unauthorized access to other systems; disseminating any discriminatory or hate-based materials or speech; or reproducing or distributing copyrighted, trademarked, proprietary, or export-controlled data or software.

e. Be in relation to sexually explicit or sexually oriented materials.

f. Refer or relate to illegal gambling, illegal weapons, and/or terrorist activities.

g. Be for the purpose of fundraising, endorsing any product or service, lobbying, or participating in any prohibited partisan political activity.

h. Be for the purpose of using applications and/or software that have not been approved by the Postal Service and that occupy or impact official computer or network processing time.

i. Result in the disclosure of any Postal Service information that is not otherwise public.

Use of Postal Service office equipment in violation or excess of the limited personal use permitted by this policy may result in limitations on future use, administrative action, criminal penalty, and personal financial liability.

For advice on how to avoid violating this policy and the corresponding misuse of government property prohibitions in the Standards of Ethical Conduct, please call the Postal Service's Ethics Helpline at 202-268-6346 or send an e-mail to *ethics.help@usps.gov*.

5-3 Electronic Mail and Messaging

Access to the Postal Service electronic mail (e-mail) system is provided to personnel whose duties require e-mail to conduct Postal Service business. If you do not comply with Postal Service e-mail policies your e-mail account may be ~~suspended~~ disabled and you will have to request your manager apply to the manager, CISO, for reinstatement of the lost privileges. Only Postal Service provided e-mail services may be accessed from Postal Service information resources. Since e-mail may be monitored, anyone using Postal Service resources to transmit or receive e-mail should have no expectation of privacy.

Sensitive-enhanced and sensitive information must be sent only to authorized personnel with a need to know and must be encrypted. Unprotected payment card industry (PCI) primary account numbers (PANs) are not to be sent via end-user messaging technology, including e-mail, chat, instant messaging, etc.

Although occasional and incidental personal e-mail use is permitted, personal messages while they remain in the system will be considered to be in the possession and control of the Postal Service.

5-3.1 Prohibited Use

Do not use Postal Service provided computing devices, including mobile devices, to check non-Postal Service (e.g., personal, supplier, contractor, and vendor) e-mail accounts (e.g., Hotmail, Yahoo, Excite, MSN) or social media. Do not use personal electronic devices to receive, process, store, or send mail containing Postal Service sensitive-enhanced, sensitive, or non-publicly available information. Other prohibited activities when using Postal Service e-mail include, but are not limited to, sending or arranging to receive the following:

a. Information that violates state or federal laws or Postal Service regulations.

b. Information designated as sensitive-enhanced or sensitive information unless encrypted according to Postal Service standards.

c. Unsolicited commercial announcements or advertising material.

d. Any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the Postal Service, the recipient, the sender, or any other person.

e. Pornographic, sexually explicit, or sexually oriented material.

f. Racist, hate-based, or offensive material.

g. Viruses or malicious code.

h. Chain letters, unauthorized mass mailings, or any unauthorized request that asks the recipient to forward the message to other people.

5-3.2 Encryption

Encrypting e-mail or messages must comply with the following:

a. Encryption software and methods must be approved by the Enterprise Architecture Committee.

b. Encryption solutions must either support key recovery or keys must be registered with authorized personnel.

c. Recovery keys or other similar files for all encrypted e-mail must be placed in a directory or file system that can be accessed by management prior to encrypting e-mail.

d. Recovery keys or other devices needed to decrypt e-mail must be provided when requested by authorized Postal Service management, the Postal Inspection Service or the Office of Inspector General.

e. Keys may not be escrowed in customer product offerings unless specifically requested in writing by the customer and approved by the executive sponsor.

5-4 Internet: Access and Prohibited Activities

Access to the Internet is available to employees, contractors, suppliers, and business partners whose duties require access to conduct Postal Service business. Since Internet activities may be monitored, all personnel accessing the Internet will have no expectation of privacy.

Prohibited activities when using the Internet include, but are not limited to, the following:

a. Downloading unauthorized content and accessing information resources outside of the Postal Service network; this includes but is not limited to using a VPN connection or attempting to bypass any Postal Service approved access technologies.

~~a.~~b. Browsing explicit pornographic or hate-based Web sites, hacker or cracker sites, or other sites that the Postal Service has determined to be off limits.

~~b.~~c. Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material the Postal Service has determined to be off limits.

~~c.~~d. Posting or sending sensitive-enhanced or sensitive information outside of the Postal Service without management authorization.

~~d.~~e. Hacking or other unauthorized use of services available on the Internet.

~~e.~~f. Posting unauthorized commercial announcements or advertising material.

~~f.~~g. Promoting or maintaining a personal or private business.

~~g.~~h. Receiving news feeds, push data updates, or continuous data streams unless the material is required for Postal Service business.

~~h.~~i. Using non-Postal Service-approved applications or software that occupy or use workstation idle cycles or network processing time (e.g., processing in conjunction with screen savers).

5-5 Prohibited Uses of Information Resources

Generally prohibited activities when using information resources include, but are not limited to, the following:

a. Stealing electronic files containing nonpublic information or copying, moving, or storing electronic files containing nonpublic information to local hard drives, removable media, or via remote-access technologies.

b. Violating copyright laws.

c. Installing unauthorized software, including games and screen savers.

d. Browsing the private files or accounts of others, except as provided by appropriate authority.

e. Performing unofficial activities that may degrade the performance of information resources, such as playing electronic games.

f. Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, and decrypt encrypted files, or compromise information security by any other means.

g. Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of, or access to, any Postal Service computer, network, or information.

h. Accessing the Postal Service network via modem or other remote access service without the approval of the manager, Corporate Information Security Office Information Security Services.

i. Promoting or maintaining a personal or private business or using Postal Service information resources for personal gain.

j. Conducting fraudulent or illegal activities including, but not limited to, gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any Postal Service or non-Postal Service computer.

k. Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.

l. Disclosing any Postal Service information that is proprietary and not otherwise public without authorized management approval.

m. Performing any act that may defame, libel or misrepresent the Postal Service, its personnel, business partners, or customers.

n. Using someone else's log-on ID and password or any other personal identity credential.

o. Using personal information resources (e.g., laptops, notebooks, personal digital assistants [PDAs], hand-held computers, or storage media including universal serial bus [USB] devices) at retail counter areas, mail processing areas, or workroom floors. This does not apply to personal information resources used by the unions in accordance with the collective bargaining agreement.

p. Connecting any non-Postal Service (e.g. personal, contractor, or supplier) information resources to the Postal Service intranet (Blue) or Postal Service computing devices.

q. The physical or wireless connection of personal mobile computing devices, such as cell phone, smart phones, tablets, and other mobile computing devices of any kind (excluding laptops) to any Postal Service network, regardless of purpose, is strictly prohibited under any circumstances.

r. Using non-Postal Service (e.g., personal, contractor, supplier) information resources to collect, process, store, transmit Postal Service sensitive-enhanced, sensitive, or non-publicly available information.

s. Plugging a Postal Service non-encrypted USB drive into a personal computing device.

t. Using unauthorized webcams, cameras, cell phones with cameras, or watches with cameras (and other personal imaging devices) in restrooms, locker rooms, retail counter areas, mail processing areas, workroom floors, vehicles, or other Postal Service areas unless approved by area or headquarters vice president or designee for business purposes. (See Management Instruction AS882-2007-6, *Postal Service Use of Retail and Cell-Phone Cameras,* on the use of handheld and cell phone cameras.)

u. Sending unprotected PANs.

v. Copying, moving, or storing cardholder data onto local hard drives or removable media when accessing cardholder information via remote access technologies.

5-6 Protection of Sensitive Data and Privacy-Related Data

Information resources must protect Postal Service sensitive data and the privacy-related data of customers, employees, and contractors in accordance with the Postal Service privacy policy and the Privacy Act as applicable. Postal Service policies related to privacy, the Freedom of Information Act, and records management can be found in Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management.* The Postal Service privacy policy for customers is posted on www.usps.com.

5-7 Sensitive Data Storage

Postal Service limits storing sensitive data to explicit business requirements. Personally Identifiable Information (PII) is prohibited from being stored for any longer than the legitimate business need exists to retain the data. Customer credit card numbers or Primary Account Numbers (PANs) should be rendered unreadable at-rest in compliance with the PCI DSS.

Supplemental Guidance: Postal Service is not required to storage of customer data for credit or debit cardholders and sensitive authentication data, after transaction authorization, is prohibited, in any form, even if it is encrypted. This includes the following data elements:

a. The full contents of any track from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere.

b. The card verification code or value three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions

c. The personal identification number (PIN) or the encrypted PIN block.

d. In the normal course of business, the following data elements from the magnetic stripe may need to be retained to minimize risk. Store only these data elements as needed for business:

1. The cardholder's name
2. Primary account number (PAN)
3. Expiration date
4. Service code

~~5-7~~ 5-8 Use of Social Media

The *Administrative Support Manual* (ASM), 363, Social Media Policy, governs the use of social media by Postal Service employees and contractors when serving the Postal Service in an official or professional capacity and provides rules and guidance for Postal Service employees and contractors who use social media for personal purposes.

6 Personnel Security

6-1 Policy

The Postal Service identifies sensitive positions and ensures that individuals assigned to those positions have the appropriate level of clearance to minimize risk to Postal Service information resources.

Personnel are held accountable for carrying out their information security responsibilities. Managers must ensure personnel receive appropriate information security training and protect Postal Service resources when personnel depart under involuntary or adverse conditions.

Policies addressed in this chapter are the following:

a. Employee accountability.

b. Sensitive positions.

c. Background investigations and clearances.

d. Information security awareness and training.

e. Departing personnel.

6-2 Employee Accountability

6-2.1 Separation of Duties and Responsibilities

Personnel must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud, or collusion.

6-2.2 Job Descriptions

The Postal Service defines and documents the information security requirements for each position.

6-2.3 Performance Appraisals

The Postal Service evaluates the execution of information security responsibilities and the compliance with information security policies and procedures in personnel performance appraisals.

6-2.4 Condition of Continued Employment

The Postal Service includes the execution of information security responsibilities and the compliance with information security policies and procedures as a condition of continued employment for all personnel.

6-2.5 Sanctions

All personnel are held accountable for carrying out their information security responsibilities. Violators of Postal Service information security policies are subject to sanctions by supervision commensurate with the severity and frequency of the infraction, including levels of access, disciplinary action, removal, or criminal prosecution.

6-3 Sensitive Positions

Managers at all levels are responsible for identifying sensitive positions within their organizations and then requesting the chief postal inspector to designate the positions as sensitive.

Sensitive positions include those in which personnel could, in the normal performance of their duties, cause material adverse effect to Postal Service information resources. Such duties include, but are not limited to, the following:

a. Making changes in the operating system, configuration parameters, system controls, and audit trails.

b. Modifying security authorizations.

c. Making revisions to sensitive programs and data that could be undetected.

6-4 Background Investigations and Clearances

6-4.1 General Requirements

Personnel must have appropriate background investigations/security clearances as determined by the Postal Inspection Service before accessing Postal Service information resources (see ASM 272, Personnel Security Clearances). For personnel without clearances, access is restricted to temporary information services (see 9-3.2.2, Temporary Information Services).

Appropriate background investigations must be conducted and security clearances obtained for personnel who access sensitive-enhanced, sensitive, or critical information resources, require unescorted access to controlled areas, or perform the duties of a sensitive position.

Personnel includes employees, nonemployees, business partners, and suppliers having access to Postal Service sensitive-enhanced or sensitive data whether that data is stored on Postal Service premises or at a business partner, supplier, or vendor facility.

6-4.2 Access Privileges

6-4.2.1 Log-on IDs

Managers must use ~~eAccessARISe~~Access/ARIS to request access authorization for individuals who do not have the appropriate clearance or background investigation and are responsible for the access activities of those individuals.

6-4.2.2 Information Resources Processing Sensitive - Enhances or Sensitive Information

All personnel whose duties require access to Postal Service information resources processing sensitive-enhanced or sensitive information (see 3-2, Information Designation and Categorization) must have an appropriate clearance or background investigation as determined by the Inspection Service before they obtain access (see ASM 272, Personnel Security Clearances).

6-4.2.3 Controlled Areas

All personnel, whose duties require unescorted access to controlled areas, whether located at a Postal or non-Postal Service facility, must have an appropriate clearance or background investigation as determined by the Inspection Service before being granted unescorted access privileges. For further information, refer to the USPS *Administrative Support Manual* (ASM), Section 272, Personnel Security Clearances.

6-4.3 Foreign Nationals

In certain situations, personnel may be permanent resident aliens and citizens of foreign countries and still provide services to the Postal Service, with prior approval of the responsible executive. Except for citizenship, foreign nationals must meet the same clearance requirements as all other personnel. The Postal Service executive who approves access to information resources by foreign nationals (including contractors and suppliers) is responsible for all actions initiated by the foreign national.

6-5 Information Security Awareness and Training

6-5.1 General Security Awareness

Managers must continually strive to incorporate information security into training courses, training videos, service talks, internal newsletters, posters, case studies, and other tools and visual aids to increase information security awareness among their personnel. The training should explain how anyone failing to comply with security policies and procedures will be disciplined.

6-5.2 Documenting and Monitoring Individual Information Security Training

Individual information security training activities must be documented and monitored to ensure all personnel attend their initial, annual, and operational training (as required) before given access to sensitive-enhanced, sensitive, or critical information.

If Postal Service-sponsored training is not available, contractors must provide appropriate information security training that is applicable to the Postal Service computing environment.

All designated personnel (see the Information Security Training Matrix on the CISO Website for the current requirements) handling PCI information must acknowledge, at least annually, in writing or electronically, that they have read and understand Postal Service information security policies and procedures contained in Handbook AS-805-C, *Information Security for General Users,* as well as the security procedures associated with their job.

6-5.3 Training Requirements

Exhibit 6-5.3

Training Requirements

Training Type	Requirement(s)
Annual Training	Based on requirements defined by the CISO at the beginning of the fiscal year (see the Information Security Training Matrix on the CISO Website), all personnel with an ACE ID or access to the Postal Service intranet must participate in information security training and data protection requirement training annually. Information security training is recommended for all other non-bargaining personnel.
Information Resource Operational Security Training	All personnel with access to the Postal Service network must be trained to handle and report information security breaches and incidents. All ~~PCI~~ developers and administrators must complete formal training [1] in general secure coding techniques, [2] in developing secure code in the programming language(s) they use, and [3] and must maintain evidence of successful completion. For information resources processing sensitive-enhanced, sensitive, or critical information, operational security training must be developed and conducted that is appropriate for job responsibilities, and role-based activities. All privileged users posing access to any sensitive-enhanced, sensitive, or critical information or systems supporting information must undergo security awareness training and records are maintained within the Learning Management System (LMS). If training does not occur, the role cannot be fulfilled. For privileged account holders who have not received annual refresher training, access is disabled until required training has been completed, unless the CISO grants a waiver. The training should explain how to protect information throughout its life cycle and report incidents. All C&A stakeholders, including Business Relationship Management portfolio managers, Solution Development Teams, and their staff must complete annual training on the Certification and Accreditation (C&A) process.

New Personnel Training	All new personnel must receive information security training and be issued a copy of Handbook AS-805-C, *Information Security for General Users.*

6-6 Departing Personnel

6-6.1 Routine Separation

Routine separation of personnel occurs when an individual receives reassignment or promotion, resigns, retires, or otherwise departs under honorable and friendly conditions. Unless adverse circumstances are known or suspected, the individual will be permitted to complete his or her assigned duties and follow official employee departure procedures. When personnel leave under non-adverse circumstances, the individual's manager, supervisor, or company official (for contractors/suppliers) must ensure the following:

a. All accountable items, including keys, access cards, two-factor credentials, laptops, tablet computers, mobile computing devices (including smart phones and encrypted storage devices) and other computer-related equipment are returned.
b. For Postal Service employee's, the employee computer log-on ID, building-access authorizations, and access to Postal Service information systems are terminated coincident with the employee's effective date of departure determined by Human Resources, unless needed in the new assignment.
c. For contractors and suppliers, their individual computer log-on ID, building-access authorizations, and access to Postal Service information systems are terminated immediately with their date of departure.
d. All sensitive-enhanced and sensitive information, in any format, in the custody of the terminating individual are returned, destroyed, or transferred to the custody of another individual.

6-6.2 Adverse Termination

Removal or dismissal of personnel under involuntary or adverse conditions includes termination for cause, involuntary transfer, and departure with pending grievances. In addition to the routine separation procedures, termination under adverse conditions requires extra precautions to protect Postal Service information resources and property. The manager, supervisor, or company official (for contractors/suppliers) of an individual being terminated under adverse circumstances must:

For Postal Service employees:

a. Ensure that the individual is escorted and supervised at all times while in any location that provides access to Postal Service information resources.
b. Immediately ~~Suspend~~ suspend and take steps to terminate the individual's computer log-on ID(s), access to Postal Service information systems, and building access authorizations.
c. Ensure prompt changing of all computer passwords, access codes, badge reader programming, and physical locks used by the individual

being dismissed.

d. Attempt to recover accountable items and all sensitive-enhanced and sensitive information in any format in the custody of the individual being terminated.
e. Attempt to wipe and/or lock any accountable item that cannot be recovered.
f. Destroy or transfer sensitive-enhanced or sensitive information to another custodian.
g. Notify the Postal Inspection Service.

Contractors and Suppliers:

a. Ensure immediate deletion of all computer passwords, access codes, badge reader programming, and physical locks used by the individual being dismissed.
b. Recover accountable items and all sensitive-enhanced and sensitive information in any format in the custody of the individual being terminated.
c. Wipe and/or lock any accountable item that cannot be recovered.
d. Destroy or transfer sensitive-enhanced or sensitive information to another custodian.
e. Immediately notify the contractor's and/or supplier's program manager (PM) or contract officer representative (COR).
f. Ensure the Contractors/Suppliers ~~eAccessARISe~~Access/ARIS account is terminated.
g. Before escorting the individual off the premises secure the Postal Service badge/ID.

6-6.3 Systems, Network, or Database Administrator Departure

Routine separation or adverse termination of a systems, network, or database administrator requires taking extra care and precautions. Upon departure, remove the privileged access as quickly as possible to maintain the security and integrity of the specific information resources to which the administrator had access. After departure, monitor the affected information resources for improper use or access. Specifically, the manager, supervisor, or company official (for contractors/suppliers) of the departing systems or database administrator must:

a. Follow the requirements documented above for routine separation or for adverse termination as applicable.
b. Reconfigure access lists to remove the departed administrator's accounts.
c. Disable or change the password or login requirements to all shared devices and applications.
d. Disable or change passwords to all shared service and privileged accounts.
e. Disallow physical access to buildings, systems, and information associated with the departed administrator's former access.

f. Monitor all privileged accounts for usage and access to the systems, applications, and databases formerly under the administrator's control to ensure all access has been removed.

g. Review records for Postal Service information approved for removal offsite and make appropriate efforts to recover information and/or equipment as applicable. Notify the manager, Corporate Information Security Office, of any information identified as removed but not recovered.

7 Physical and Environmental Security

7-1 Policy

The Postal Service protects its information resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorized personnel.

Where possible, all information resources (including portable information resources) must reside in a protected environment. Physical and administrative security controls must be implemented at each facility to protect against unauthorized personnel access and to protect the physical integrity of Postal Service information resources located at the facility. Such physical and administrative security controls include the following:

a. Physical access controls.

b. Physical protection of information resources.

c. Environmental security.

d. Facility continuity planning.

e. Facility contracts.

7-2 Physical Access Controls

7-2.1 Access to Controlled Areas

Access to controlled areas must be restricted as follows:

a. Access to controlled areas is restricted to personnel whose duties require access to such facilities and who possess appropriate security clearances or background investigation.

b. Access to controlled areas must be controlled by electromechanical means. Personnel authorized access to the controlled areas must always use their access control identification badge or device to gain entrance to the controlled area. Tailgating is prohibited and personnel are responsible for immediately reporting any instance of tailgating.

c. A record of physical access, both authorized individuals and visitors, must be maintained. Automated mechanisms should be employed where feasible to facilitate the maintenance and review of access records.

d. Personnel without an authorized Postal Service identification badge or device must sign a visitor log and be escorted by authorized personnel while in the controlled area.

e. Visitor logs must include at a minimum: name and organization of the person visiting, form of identification used for authentication, date of visit, time of entry and departure, purpose of visit, and name of person and organization visited. Visitor logs must be reviewed monthly and security violations and suspicious activities must be investigated and remedial actions taken.

7-2.2 Establishment of Controlled Areas

Controlled areas must be established within the facility wherever more stringent restrictions on physical access and more tightly controlled physical and environmental security are required to fully protect information resources. Typical controlled areas may include the following:

a. Computer rooms.

b. Telecommunications rooms.

c. Wiring closets.

d. Computer operations areas.

e. Media and documentation storage areas.

f. Operating system software support areas.

g. Special authorization terminal areas.

h. Security officers' controlled areas.

i. Other designated areas, whether located at a Postal Service or non-Postal Service facility.

7-2.3 Types of Information Resources Stored in Controlled Areas

Information resources processing sensitive-enhanced, sensitive, or critical information must be located in a controlled area.

7-2.4 Establishment of Access Control Lists

Each controlled area must establish an access control list of people who are authorized access. Access control lists must be updated when new personnel are assigned to the controlled area or when someone leaves. Access control lists must also be reviewed and updated semiannually. Data center access must be reviewed by the designated Information Technology manager on a quarterly basis.

Personnel not on the access control list must sign a visitor log and be escorted by authorized personnel while in the controlled area.

7-2.5 Training for Controlled Areas

Personnel with access to controlled areas must be trained in their responsibilities regarding controlled areas.

7-2.6 Installation of Physical Access Control Devices

Physical access control devices using biometrics, smart cards, tokens, mantraps, or lockable cabinets may be installed to supplement traditional facility locks and keys to limit access. Additionally, the Inspection Service and Facility Management may require physical access to be monitored by surveillance equipment and real time intrusion detection and alarm systems (e.g., CCTV, motion detectors, and other audio or silent alarms) to detect and respond to incidents [see the *Administrative Support Manual* (ASM) 273, Facility Security, and Handbook RE-5, *Building and Site Security Management*].

Based on the risks associated with the information resource, additional physical access security mechanisms (e.g., locked cabinet or desk, portable device cable lock, and biometric workstation lock) must be implemented for information resources processing sensitive-enhanced, sensitive, or critical information.

Security personnel are notified immediately of physical security events and follow-up action is taken and documented.

7-2.7 Implementation of Identification Badges

Identification badges must adhere to the following criteria:

a. Persons authorized access to controlled areas must be identified by a picture badge conspicuously displayed on their person.

b. Persons using a badge not issued to them or making any attempt to alter a badge will be subject to disciplinary action.

c. Employees must report lost or stolen badges immediately to the issuer of the badge.

d. Security access systems that limit access to controlled areas where persons have reported lost or stolen badges must immediately cancel the associated access privileges until the lost or stolen badge is recovered and returned to the issuer.

e. Temporary badges must be controlled and issued by the manager of the organization or their designee to authorized personnel who arrive without their assigned badges during normal duty hours.

f. The organization manager or designee must make an unannounced verification of badges at least annually to ensure authenticity and to correct any badge discrepancies.

7-3 Physical Protection of Information Resources

Information resources must be protected against damage, unauthorized access, and theft, both in the Postal Service environment and when removed from this secure environment.

Note: Sensitive-enhanced, sensitive, and critical information stored on removable devices or media must be encrypted and stored in a controlled area or in a locked cabinet. Sensitive-enhanced and sensitive information that is stored off Postal Service premises must also be encrypted and stored in a controlled area or in a locked cabinet.

7-3.1 Network Equipment, Network Servers, and Mainframes

Network equipment, network servers, and mainframes must be protected against damage, unauthorized access, and theft and, where possible, housed in separate rooms that can be accessed only by authorized personnel.

Additional protection measures to control physical access to information distribution and transmission include locked wiring closets, disconnected or locked spare jacks, and protection of cabling with conduit or cable trays.

7-3.2 Postal Service Workstations and Portable Devices

Postal Service information resources that are stationary, portable, or mobile must be protected at all times in use, storage, and in transit against damage, unauthorized access, and theft. Users of Postal Service information resources will be held accountable for their loss or compromise.

7-3.3 Non-Postal Service Portable Electronic Devices

To protect Postal Service information from disclosure or compromise, non-Postal Service portable devices [e.g., laptops, notebooks, tablets, mobile computing devices, or storage media including universal serial bus (USB) port devices or thumb drives] must not store, process, or transmit Postal Service information. Under no circumstances will such devices connect to the Postal Service intranet via a wired or wireless connection.

The use of non-Postal Service portable devices for personal use is controlled by rules set forth by the installation head or his or her designee.

Visitors to Postal Service facilities may be required to present non-Postal Service portable devices to the installation head or his or her designee upon entry to the facility. The installation head or his or her designee determines if such devices can be brought into the facility or must be surrendered for the duration of the visit. Under no circumstances will such devices connect to the Postal Service intranet or store, process, or transmit Postal Service information.

7-3.4 Sensitive-Enhanced, Sensitive, and Critical Media

Sensitive-enhanced, sensitive, and critical media, whether electronic or non-electronic, must be protected against physical loss or damage, whether on Postal Service premises or not. Physical and administrative controls must be implemented to ensure that only authorized personnel can access sensitive-enhanced, sensitive, and critical information. Personnel who have custody of sensitive-enhanced, sensitive, and critical media are responsible for their safekeeping (see 3-5, Protection of Postal Service Information and Media).

7-3.5 Contracts

Physical security requirements must be included in contracts involving infrastructure services performed or hosted for the Postal Service.

7-4 Environmental Security

Environmental security controls must be implemented at the facility, room, and information resource level to protect servers, mainframes, and critical information resources as described below:

a. Protection against lightning, wind, and building collapse must be implemented.

b. Protection against water damage from water supply lines, sewer systems, and roof leaks must be implemented (e.g., plastic sheets are available and master shutoff valves are accessible, working properly, known to operations personnel, and automatic where feasible).

c. Additional temperature and humidity safeguards must be implemented to monitor and maintain acceptable levels.

d. Protection against flooding, earthquakes, or other natural disasters must be implemented (e.g., drains are installed below the computer room floor).

e. Additional fire safeguards:

   (1) Fire detection and suppression equipment (e.g., smoke and heat detectors, handheld fire extinguishers, fixed fire hoses, and sprinkler systems) must be implemented.

   (2) Fire detection and suppression equipment must automatically notify the organization and emergency responders.

f. Additional power (electricity) safeguards:

   (1) A short-term alternate power supply must be implemented to ensure proper shutdown in the event of a power interruption.

   (2) A long-term alternate power supply must be implemented to maintain minimal operational capability in the event of a power outage.

g. Automatic emergency lighting systems must be implemented to illuminate emergency exits and evacuation routes in the event of a power outage or disruption.

h. Surge protection must be implemented for all information resources.

i. Redundant power feeds and redundant communications paths must be implemented for critical information technology sites.

For areas containing concentrated information resources, Facility Management may require the capability to shut off power to information resources that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to potential flooding) without endangering personnel by requiring them to approach the equipment. See ASM 273, Facility Security, and Handbook RE-5, *Building and Site Security Management,* for the requirements for remote power shutoffs.

7-5 Facility Continuity Planning

Physical security requirements must be included in facility continuity planning to ensure the appropriate protection of information resources following a catastrophic event.

7-6 Facility Contracts

Depending on the nature of the contract, information, environmental, personnel, and physical security requirements must be included in contracts involving facilities to ensure the appropriate protection of information resources.

8 Development and Operations Security

8-1 Policy

Information resources must be developed under the technical solutions life cycle (TSLC) or other approved system development life cycle methodology. Information security must be an integral part of the system development life cycle whether development is done in house, acquired, or outsourced. Postal Service information must also be appropriately protected during operation. Security activities must be performed to maintain a secure environment and to comply with Postal Service policies and legal requirements.

The Postal Service certification and accreditation (C&A) process defines a formal review process that ensures adequate security is incorporated during each phase of the project life cycle. The C&A process is required for each information resource (i.e., application or infrastructure component).

Chapter 8 addresses the following topics:

a. Development security.

b. Operations security.

c. Certification and accreditation.

8-2 Development Security

8-2.1 Life-Cycle Approach

Security must be addressed throughout the information resource life-cycle process, from requirements, design, build, system integration testing (SIT), customer acceptance testing (CAT), release (and production) and retirement. All development, acquisition, or integration projects for information resources,

whether performed in house or by a business partner, must follow the TSLC process or other approved systems development life-cycle methodology. All systems development must follow secure coding best practices.

8-2.2 Risk Management

A risk-based approach must be applied to information security that uses limited resources wisely to protect an information resource in a cost-effective manner throughout its life cycle. The security controls applied to information resources must be commensurate with the magnitude of harm that would result from loss, misuse, unavailability, unauthorized access, or unauthorized modification of the information resources (see 4-3, Information Resource Risk Management).

8-2.3 Quality Assurance

Information resource development must include quality assurance (QA) and security-specific testing to ensure that security controls have been implemented and are functioning correctly. Transactions failing edit and validation routines must be subject to appropriate follow-up until errors are remediated. Information processing failures discovered as the result of remediation must be used for root cause analysis and to adjust procedures and automated controls to improve quality.

8-2.4 Configuration and Change Management

All information resources, whether developed in house, outsourced, or acquired must be developed under standard configuration and change management procedures to maximize risk reduction and vulnerabilities introduced by undocumented and untested changes in accordance with the Postal Service change management policy/procedure. Postal Service information resources must not be developed or deployed unless a change and configuration management process is in place.

Configuration and change control involve the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. Appropriate organizational officials approve information system changes in accordance with this process. Emergency changes are also included in the configuration and change control process.

8-2.4.1 Configuration Component Inventory

To effectively manage information resources, the information system components must be inventoried and the initial or baseline configuration of the information resources must be documented in the corporate Configuration Management Database (CMDB) prior to deployment. The inventory of information system components must include manufacturer, type, serial number, version number, information system/component owner, and location (i.e., physical location and logical position within the information system architecture). The inventory must also designate those information system components required to implement and/or conduct contingency planning operations.

Configurations of information resources must be reviewed at least annually to ensure the documented configuration in the appropriate inventory application matches the current components.

8-2.4.2 Configuration Hardening Standards

Hardware and system software must be hardened to Postal Service information security requirements. Configuration hardening standards must be used to maintain a high level of information security, enable cost-effective and timely maintenance and repair, and protect Postal Service information resources against unexpected vulnerabilities. Critical security patches for PCI-related information resources, including applications and infrastructure, must be installed within 30 days of release. See the manager, Corporate Information Security Office (CISO) ~~Information Security Services (ISS)~~, to request access to a specific Postal Service configuration hardening standard.

Secure System Configuration: Software developers and COTS software suppliers must provide secure configuration guidelines that fully describe all security relevant configuration options and their implications for the overall security of the software and system.

a. The guideline shall include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security.

b. Developers must determine how to configure each setting that has an effect on security so the default configuration settings are secure and they do not weaken the security functions provided by the platform, network infrastructure, or services.

8-2.4.3 Change and Version Control

Changes to information resources and configurations must be managed to ensure that Postal Service information resources are not inadvertently exposed to unnecessary risks and vulnerabilities and that only qualified and authorized individuals initiate changes, upgrades, and modifications. Individual access privileges must be approved by appropriate management officials.

All changes must be appropriately approved and documented. Application code changes are managed using version control software. Change control records must be maintained to support and document system software maintenance, software and hardware upgrades, and any local system modifications.

8-2.4.4 Patch Management

An effective patch management process must be implemented to investigate, prioritize, test, track, control the deployment and maintenance of software releases, and resolve known security vulnerabilities. The patch management process must address all information resources installed in the Postal Service computing environment. Security patches must be installed in accordance with the agreed upon schedule and following established evaluation and implementation processes. Critical security patches for PCI- related information resources, including applications and infrastructure, must be installed within 30 days of release. Software security patches must be evaluated on a regular basis. The evaluation period varies by platform and is defined in the applicable hardening standard. If the patch is appropriate for the Postal Service environment, the patch must be tested and approved by Postal Service management prior to implementation. Software patch

evaluations and testing must be properly documented and retained in the appropriate repository that is available for audit purposes. Personnel involved in the patch management process must be appropriately trained to ensure a viable vulnerability remediation process.

Patch management involves acquiring, testing, and installing multiple patches (code changes) to software systems, including operating system software, supporting software and packages, firmware, and application software. Patch management tasks include the following:

a. Maintaining current knowledge of available patches.
b. Deciding what patches are appropriate for particular information resources.
c. Prioritizing the patches to be installed.
d. Testing patches in a nonproduction environment first in order to check for unwanted or unforeseen side effects.
e. Developing a back-out plan which includes backing up the systems about to be patched to be sure that it is possible to return to a working configuration.
f. Securing management approval.
g. Ensuring that patches are installed properly.
h. Testing information resources after installation.
i. Documenting all associated procedures, such as specific configurations required.

Patch management is critical to ensure the integrity and reliability of information resources. Patch management should be capable of:

a. Highly granular patch update and installation administration (i.e., treating patches and mainframes, servers, desktops, and laptops separately).
b. Tracking machines, and updating and enforcing patches centrally.
c. Verifying successful deployment on each machine.
d. Deploying client settings, service packs, patches, hot fixes, and similar items network-wide in a timely manner in order to address immediate threats. Critical security patches for PCI-related information resources, including applications and infrastructure, must be installed within 30 days of release.
e. Initiating from a central management console.
f. Providing scheduling, desktop management, and standardization tools to reduce the costs associated with distribution and management.

g. Providing ongoing deployment for both new and legacy systems in mixed hardware and operating system environments.

h. Automating the repetitive activity associated with rolling out patches.

i. Analyzing the operating system and applications to identify possible security holes.

j. Scanning the entire network (IP address by IP address) and providing information such as service pack level of the machine, missing security patches, key registry entries, weak passwords, users and groups, and more. For MPE and MHE systems, a scan schedule must be reviewed with system owners to prevent needless negative impact to mail processing and logistics operations.

k. Analyzing scan results using filters and reports to proactively secure information resources (e.g., installing service packs and hotfixes).

8-2.4.5 Security Testing of the Configuration

After the information system is changed, the security controls must be checked to ensure the security features are still functioning properly. Periodically (at a minimum annually), the security controls must be tested to ensure the information security controls are functioning as designed and documented.

Significant changes will cause the re-initiation of the C&A process. The criteria for initiating a recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process,* 6-2.

8-2.5 Separation of Duties

An individual or organization must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for accidental or malicious wrongdoing, fraud, or collusion. When it is not possible for duties to be assigned to separate individuals, the roles and functions performed must be clearly defined, associated activities logged, security-related functions audited, and compensating controls identified and implemented. The CISO reserves the right to validate the effectiveness of the compensating controls.

8-2.6 Application Source Code

Application source code is considered business proprietary information by the Postal Service and is expected to be handled and stored in a secure manner. When source code is consolidated and stored in a repository/vault, that repository/vault is considered sensitive and must adhere to the following controls:

a. The repository/vault must be in a controlled area and physical access to the repository/vault will be controlled through an access control system.

b. Electronic access to the repository/vault will be controlled through ~~eAccess~~ARISeAccess/ARIS.

c. A fully accountable check-in/check-out process must be operational.

d. Code may not be removed from the vault without using the approved check-in/check-out process.

e. Any code that is removed from the vault must be protected from unauthorized access or usage.

f. Business partners having access to code must have a valid Postal Service nondisclosure agreement (NDA) on file with the Postal Service. Business partner NDAs will be filed with the contracting officer.

g. A defined process of separation of duties must be implemented to support code propagation through the environments (e.g. developers will not have the ability to place code directly into the production environment).

h. A versioning system must be in-place to ensure that proper version control is maintained.

8-2.7 Developers

A developer is an employee or contractor with the development-related responsibilities (e.g., the ability to check-in code or make changes to source code, scripts, or configuration files) and as such must be included in the Postal Service Corporate Developer Registry (CDR).

The following restrictions apply to all developers:

a. Developers are not authorized to be production application/platform administrators.

b. Developers are not authorized to copy production data.

c. Developers are not authorized to have greater than read access to the underlying operating system.

d. Developers are not authorized to have greater than read access to the underlying database.

e. Developers are not authorized to have greater than read access to the application (i.e., under no circumstances are developers ever allowed to have privileged or administrative access to the application).

f. Developers are not authorized to promote code to the production environment.

g. The definition of developer is global in scope, and these restrictions apply across all applications and platforms.

8-2.8 Application Security

To address today's threat environment, developers must employ some of the new application controls that are harder to evade and more effective than many of the traditional security controls currently employed.

8-3 Operations Security

8-3.1 Distributed Postal Computing Environment

The TSLC defines the following four logical distributed postal computing environments (PCE) as follows:

a. Development (DEV). DEV includes subcategories Sandbox and Inactive.

b. System Integration Testing (SIT).

c. Customer Acceptance Testing (CAT). CAT includes subcategories Training, Quality Assurance (QA), and Pre-Production (Pre-Prod).

d. Production (PROD). PROD includes subcategories Pilot, Certification, Testing Environment for Mailers (TEM), and Disaster Recovery (DR).

The use of any other PCE name or subcategory is not authorized. National systems/applications must be engineered with a minimum of three separate environments with appropriate separations of duties. The three separate environments must have at least four logical environments that are DEV, SIT, CAT, and PROD. In a three-separate environment approach, the acceptable groupings of these four logical environments in the three separate environments are DEV/SIT, CAT, PROD or DEV, SIT/CAT, PROD. In the latter grouping, the SIT environment must be cleared before it becomes the CAT environment.

8-3.2 Environment Restrictions

Restrictions are defined for the following distributed PCEs including the subcategories noted above:

a. DEV.

b. SIT.

c. CAT.

d. PROD.

Separation of duties and other restrictions defined for each of the PCEs must be maintained. Modification of environment restrictions is not authorized.

8-3.2.1 Development Environment

Developers get full access (e.g., read, write, execute, allocate, and delete) in this environment to application software. Restrictions for the development environment include the following:

a. Developers are restricted to read and execute privileges for database and operating system software.

b. Personally identifiable information (PII), which is defined in 3-2.4.2, and payment card industry (PCI) primary account number (PAN) must not be used in this environment.

c. No access to production systems is allowed from this environment.

d. Development environment is an isolated infrastructure (DEVSUB) or enclaved.

e. Use of non-sensitive production information in this environment requires the creation of a generic production data usage letter (PDUL). This letter approves the use of non-sensitive production data until the end of the current fiscal year. The PDUL is needed only for the application to be tested not for every system the application touches.

f. Use of sensitive or sensitive-enhanced production information in this environment requires:

(1) A specific PDUL that approves the use of this data ~~until the end of the current fiscal~~ for (1) one year from the time of the request, at which time another PDUL will be required. The PDUL is needed only for the application to be tested, not for every system the application touches.

(2) The development environment must implement the same controls as the production environment or the PII or PCI PANs, and sensitive information must be de-identified in the production environment before data is transferred to the development environment. The project manager must validate (and attest in a letter to the CISO and the privacy office) that all PII and PCI PANs, and sensitive information have been de-identified.

g. All connections of developer workstations to databases in all environments must be added as a temporary request for no more than 6 months with the option to renew when the NCRB team (coordinating with

the ISSO) contacts the requester prior to expiration; contact the users listed in the database connections in the general tab of ServiceNow. This fits the 6-month access review policy.

h. All connections for developers will be from their workstations/laptops and not from a subnet.

8-3.2.2 SIT Environment

Developers have full access (e.g., read, write, execute, allocate, and delete) in this environment to application software. Code is migrated from the SIT environment back to the development environment to apply updates/fixes. Restrictions for the SIT environment include the following:

a. Developers may have access to the SIT environment with documented management approval.

b. Systems moved to the SIT environment are documented and managed by a version control library system.

c. PII and PCI PANs and sensitive information must not be used in this environment.

d. Use of non-sensitive production information in this environment requires a generic PDUL that approves upfront the use of non-sensitive production data for up to 1 year from the time of the request until the application requires recertification and reaccreditation at which time another PDUL will be required.

e. Use of production PII and PCI PANs, and sensitive information in this environment requires:

(1) A specific PDUL that approves the use of this data for 1 year from the time of the request; then they would be required to request another PDUL. The PDUL is only needed for the application to be tested not for every system the application touches.

(2) The SIT environment must implement the same controls as the production environment or the PII, or PCI PANs, and sensitive information must be de-identified in the production environment before the data is transferred to the SIT environment. The project manager must validate (and attest in a letter to the CISO and the privacy office) that all PII, and PCI PANs, and sensitive information have been de-identified.

f. All connection of developer workstations to databases in all environments must be added as a temporary request for no more than 6 months with the option to renew when the NCRB team (coordinating with the ISSO) contacts the requester prior to expiration; contact the users listed in the

database connections in the general tab of ServiceNow. This fits the 6-month access review policy.

g. All connections for developers are from their workstations/laptops and not from a subnet.

8-3.2.3 CAT Environment

Access is restricted to production operations personnel, executive sponsorship, and developers with proper authorization. The CAT environment must implement the same controls and security requirements as production. Restrictions for the CAT environment include the following:

a. Developers may have access to the CAT environment with documented management approval.
b. Systems moved to the CAT environment are documented and managed by a version control library system.
c. PCI PANs must not be used in this environment.

d. PII and sensitive information must be de-identified prior to use in the CAT environment; any exceptions to the de-identification requirement must be approved by the CIO, CPO, and the executive sponsor. If PII that is not de-identified is approved for use in the CAT environment, the PII and sensitive information must be encrypted.
e. Use of non-sensitive production information in this environment requires a generic PDUL that approves upfront the use of non-sensitive production data for up to 1 year from the time of the request until the application requires recertification and reaccreditation at which time another generic PDUL is required. See 8-3.2.5, Other Environments.
f. Use of PII, and PCI PANs, sensitive information in this environment requires:

(1) A specific PDUL that approves the use of this data ~~until the end of the current fiscal~~ for (1) one year from the time of the request, at which time another PDUL is required. The PDUL is only needed for the application to be tested, not for every system the application touches.

(2) The CAT environment must implement the same controls as the production environment or the PII and PCI PANs, and sensitive information must be de-identified in the production environment before data is transferred to the CAT environment. The project manager must validate and attest in a letter to the CISO and the Privacy Office that all PII and PCI PANs, and sensitive information have been de-identified.

(3) All connection of developer workstations to databases in all environments must be added as a temporary request for no more than 6 months with the option to renew when the NCRB team (coordinating with the ISSO) contacts the requester prior to expiration; contact the users listed in the database

connections in the general tab of ServiceNow. This fits the 6-month access review policy.

(4) All connections for developers will be from their workstations/laptops and not from a subnet.

8-3.2.4 Production Environment

Restrictions for the production environment include:

a. Developers must not have ongoing read access or privileged access to application, database, and operating system software in this environment.

b. Developer access to production systems must be authorized by the executive sponsor, CIO or designee, and CPO via ~~eAccess~~ARIS~~e~~Access/ARIS or PS Form 1357, *Request for Computer Access*. PS Form 1357 is only to be used for applications where ~~eAccess~~ARIS~~e~~Access/ARIS is unable to handle the requested computer access.

c. Developer access to the production system, if approved in ~~eAccess~~ARIS~~e~~Access/ARIS, must be managed and documented in ~~eAccess~~ARIS~~e~~Access/ARIS.

d. A Remedy Problem Ticket must be opened to implement the approved access to the production system and the access must be removed when the Problem Ticket is closed.

e. The developer account must be temporary and disabled/removed upon completion of the task.

f. Developer access must be logged while the account is active.

g. The CISO must be informed of the access.

h. Production data must not be copied by the developer.

i. Extreme care must be exercised when accessing PII and cardholder information. If not necessary for the task, PII and cardholder data must be masked from view or de-identified. Masking is the method of concealing portions of cardholder data when displayed or printed. De-identifying production data is the process of systematically transforming PII and cardholder data elements so they can no longer be used identify an individual or cardholder data. When masking the PAN, the first six and the last four digits are the maximum number of digits to be displayed or printed.

j. Sensitive and sensitive-enhanced information must be protected according to the requirements in 3-5.

8-3.2.5 Other Environments

The restrictions are the same as for the development environment.

8-3.3 Testing Restrictions

All information resources must comply with the testing restriction policies below.

The SIT and CAT environments must be representative of the operating landscape, including likely workload stress, operating system, application software, database management systems, and network/computing infrastructure found in the production environment. As the production environment changes, the test environment must also change to stay in synchronization.

The testing must only be conducted within the CAT environment by a test group independent from the development team using clearly defined test instructions (scripts) and interactive testing that adequately address the testing requirements and success criteria defined in the test plan. Errors found during testing must be logged, classified (e.g., minor, significant, and mission critical), and communicated to key stakeholders.

8-3.3.1 Development and Testing in the Production Environment

Development and testing of hardware and software must not be performed in the production environment. Engineering development and testing are in the production environment except as planned and implemented by MPE/MHE.

8-3.3.2 Testing With Non-sensitive Production Data

Prior approval in writing is required from the executive sponsor and CIO or designee if non-sensitive production data is to be used in a test environment, regardless of where the testing is conducted. Such approved production data files must be identified as "copies" to prevent them from being reentered into the production environment.

8-3.3.3 Testing with Sensitive-Enhanced and Sensitive Production Data

Prior approval in writing is required from the CPO, executive sponsor, and CIO or designee if sensitive-enhanced and sensitive information is to be used in a test environment, regardless of where the testing is conducted. Approved data files must be identified as "copies" to prevent them from being re-entered into the production environment.

Prior to usage of production data in a test environment, the test environment must be hardened to production standards.

PII or cardholder data must not be placed in the test environment without being de-identified. The masked/transformed data elements must then be propagated across related tables within the database to preserve the integrity of data relationships, maintain the referential integrity of the test data, and ensure the validity of test results.

8-3.3.4 Testing at Non-Postal Service Facilities with Production Data

Additional approval in writing is required from the manager, CISO, if production data is to be used in a test environment outside of Postal Service facilities.

Such approved files must be identified as "copies" to prevent them from being re-entered into the production environment.

8-3.4 Compensating Controls in lieu of Production Data Usage Letters

The following compensating controls must implemented in lieu of Production Data Usage Letters (PDULs):

a. Current ~~eAccessARISe~~Access/ARIS approvals for accessing production data in a nonproduction environment.

b. Information resource used to access this data must have a content management solution deployed that restricts the removal of PII and PCI cardholder information from the information resource.

c. Information resource used to access this data must have an encryption solution that meets Postal Service standards.

d. Users must shut down the information resource before leaving for the day.

e. Data masking must be implemented, where feasible, on development and test servers to protect PII and PCI cardholder information. Masking must be performed in a manner that does not expose the original file to unauthorized access and must be appropriately destroyed after the masked data version is created.

f. If data is transferred to an end point information resource, the transport method must employ an encryption solution that meets Postal Service standards.

g. Users must be on Postal Service premises for these compensating controls to be applicable; these compensating controls are not sufficient for remote off-site access.

h. Information resources engaged in accessing production data in a nonproduction environment are subject to 'data at rest' scans.

8-4 Certification and Accreditation

C&A is a formal security analysis and management approval process to assess residual risk before the resource is put into production. Each phase of the TSLC has corresponding security activities that must be performed to maintain a secure environment and comply with Postal Service policies and legal requirements. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for more details.)

8-4.1 **What the C&A Process Covers**

The C&A process consists of ~~seven~~ (9) nine interrelated phases that are conducted concurrently with the development and deployment of new information resources. The objectives of the C&A are to assess threats, define security requirements and controls, test security solutions, and evaluate the security controls and processes chosen to protect the information resource.

Sensitive-enhanced, sensitive, critical-high, and critical-moderate information resources must complete the C&A process culminating with the ~~certification, accreditation, and approval to deploy~~certification ad accreditation of the information resource. ~~All three~~Both approvals (i.e., ~~certification, accreditation, and approval to deploy~~certification and accreditation) are required before beginning operations.

All wireless information resources, regardless of sensitivity or criticality, must complete the C&A process.

8-4.2 **When C&A Is Required**

The C&A is required for the following:

a. All information resources, regardless of whether they are located at a Postal Service or non-Postal Service facility or whether they are controlled directly by the postal Service or through a contractor or business partner.

b. All wireless information resources, regardless of sensitivity or criticality, must complete the C&A process.

~~b.~~c. Pilot projects or proof of concept for information systems prior to processing production or live data.

The frequency for recertification and reaccreditation is defined in the Re-Initiate C&A section. Refer to section 8-5.8.8 Reinitiate C&A

~~8-4.2.1~~ Interim Authority To Test

An IATT is a temporary authorization to test an information resource within any owned or operated Postal Service information environment. The information environment of interest will process, store, or collect Postal Service data under a short time frame per a predetermined set of conditions or constraints. An IATT may also be used to field new systems or capabilities for a limited time (such as Proof of Concept), with a limited number of platforms to support developmental efforts, demonstrations, or exercise.

*Note: An IATT is **only** required if an information resource meets the conditions explained above. An IATT is not required for every information resource.*

IATTs are granted for a limited duration of either 30, 60, or 90 days with an option for one extension. The IATT process may not be used to avoid authorization or validation activity and certification determination requirements for authorizing a system to operate.

It is Postal Service policy that all information systems, applications and services (referred to collectively as (information system (IS)) will be certified through the appropriate Postal processes as identified in Handbook AS- 805-A. All uncertified ISs that are to be fielded for a limited time (such as a Proof of Concept), with a limited number of platforms to support developmental efforts, demonstrations, or exercise shall receive an IATT prior to connecting to a live (production) network. ISs receiving an IATT will not be used for operational activities; the IATT is granted for testing purposes and to support demonstrations and exercises. This testing may include limited user testing, independent validation and verification testing to facilitate Postal Service certification.

8-4.3 Value of C&A Process to the Postal Service

C&A demonstrates that the Postal Service has taken due care to protect its information resources in accordance with policies and legal requirements defined by its business, legal, and administrative entities and ensures that the security measures implemented to protect such resources are documented.

8-4.4 Access to Information Resources and Related Documentation

During the C&A process, the manager, CISO, or designated agent has unrestricted access to the information resources and related documentation.

8-4.5 Independent Processes

Independent processes are evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information resources. The following independent processes may be conducted by an organization that is separate and distinct from those responsible for the development and operation of the information resource and that strictly adheres to the separation-of-duties policy:

a. Independent risk assessment.

b. Independent security code review.

c. Independent penetration testing and vulnerability scans.

d. Independent security test validation.

Additional information is available in Handbook AS-805-A, *Information Resource Certification and Accreditation Process.*

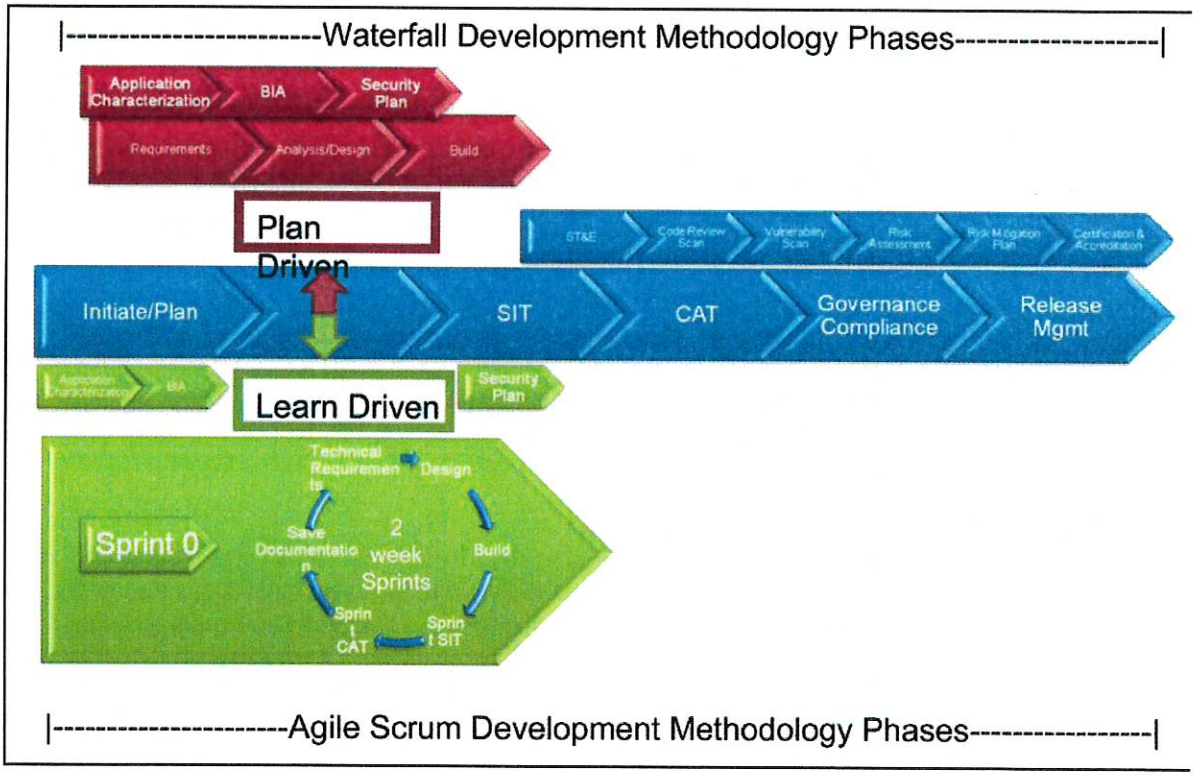
8-4.6 Contractual Terms and Conditions

Contract language and partnering agreements must reflect the information security requirements of the Postal Service defined in the C&A process. The executive sponsor is responsible for ensuring that the security requirements are included in all contracts that involve developing information resources and all contracts with businesses that transmit information to or from trusted Postal Service networks.

8-5 Information Resource C&A

Exhibit 8-5 depicts the seven phases of the Waterfall and Agile Scrum Development Methodologies and the major documents (deliverables) for each phase. The information security activities associated with the C&A phases are described in the following paragraphs.

Exhibit 8-5
Seven C&A Phases



8-5.1 Phase 1 — Initiate and Plan

Phase 1 determines what will be required during the C&A and the magnitude of the effort needed to complete the C&A process. The process is initiated for all information resources regardless of their location or whether they are controlled directly by the Postal Service or through a contractor or business partner. Information resources may be referred to as a technical solution within the TSLC. The C&A process can be applied to pilot, new, and production applications, infrastructure, and business partner initiatives.

8-5.2 Phase 2 — Requirements

Phase 2 determines the information security requirements and begins to assess the risks. The information security activities of Phase 2 are described in the following paragraphs.

8-5.2.1 Conduct Business Impact Assessment

An Impact Assessment is completed to determine the level of sensitivity and criticality and the information security requirements for the information resource.

8-5.2.1.1 Determine Sensitivity and Criticality

The Privacy Impact Assessment is completed followed by the determination of sensitivity and criticality for all information resources.

8-5.2.1.2 Determine Security Requirements

Security requirements are defined for all information resources to secure the information resources commensurate with the risk. Security requirements include the following:

a. Baseline security requirements for all information resources.

b. Additional security requirements based upon the sensitivity and criticality of the information resource, legislation, regulations, directives, and industry requirements.

c. Additional conditional requirements based on request by senior management or specific criteria.

d. Additional security requirements recommended by the information system security officer (ISSO) based on generally accepted industry practices, the operating environment, and the risks associated with the information resource.

8-5.3 Phase 3 — Design

Based on the security requirements defined in the BIA, the security controls and processes for the information resource are defined. The information security activities of Phase 3 are described in the following paragraphs.

8-5.3.1 Develop High-Level Architecture

A high-level architectural diagram is developed and maintained current for all information resources documenting hardware, communication services and ports used, security devices, and interconnected resources. The architectural diagram is used by the manager, CISO ISS to determine the impact on the infrastructure and the need for additional security controls such as an enclave (see 11-3.7, Determining When a Secure Enclave Is Required).

8-5.3.2 Identify Internal and External Dependencies

Internal and external dependencies must be identified and documented in the eC&A process.

8-5.3.3 Document Security Specifications

If information resource is contracted, security specifications are documented to satisfy the security requirements defined by the BIA.

8-5.3.4 Select and Design Security Controls

Identify potential security controls (safeguards) based on the information security requirements and in light of business requirements including project schedule and budget.

An analysis of potential controls is conducted to determine their potential effectiveness to remove, transfer, or otherwise mitigate risk to information resources. The controls analysis identifies any residual risk to the information resource.

A cost-benefit analysis is performed and documented to facilitate the implementation of cost-effective protection for information resources.

Safeguards are selected or designed based on the controls analysis and the cost-benefit analysis.

8-5.3.5 Develop Security Plan

A security plan must be developed for all information resources. A security plan is a blueprint for designing, building, and maintaining an information resource that can be defended against threats, including intruders, both internal and external. The security plan covers both the nonproduction and production environments and describes all information security controls that have been implemented or planned.

8-5.3.6 Conduct a Site Security Review

The site security review assesses the physical security controls of facilities hosting sensitive-enhanced, sensitive, and critical information resources. The lack of adequate physical security controls could affect the availability, confidentiality, and integrity of Postal Service applications and the information resources hosting them. A site security review may not be required if the site is accredited by a government agency.

Site security reviews of non-Postal sites storing PCI cardholder information must be conducted annually but should be conducted more frequently if it is deemed there is increased risk.

The site security review results in a report and not a Postal Service certification or accreditation.

8-5.4 Phase 4 — Build

The security controls and processes selected and defined in Phase 3 for the information resources are implemented in this Phase. The information security activities of Phase 4 are described below.

8-5.4.1 Develop, Acquire, and Integrate Security Controls

Appropriate security controls are developed in house, acquired, or outsourced depending on the cost-benefit analysis and integrated into the information resources and related processes.

8-5.4.2 Hardening Information Resources

Information resources hosting sensitive-enhanced, sensitive, and critical applications and information resources that are part of the Postal Service infrastructure must be hardened to meet or exceed the requirements documented in Postal Service hardening standards. Hardening refers to the process of implementing additional software, hardware, or physical security controls. Hardening standards are based off of Center of Internet Security (CIS) sources, vendor recommended setting and industry best practices. If a benchmark is not developed by CIS sources, vendor recommended security settings are established by the Postal Service.

8-5.4. Develop Security Operating Procedures

Security operating procedures for emergencies, separation of duties, secure computer operations, manual processes, etc., must be developed for all information resources.

8-5.4. Develop Operational Security Training

Appropriate materials are developed for training users, system administrators, managers, and other personnel on the correct use of the information resource and its security controls.

8-5.4.5 Incorporate Security Requirements in Service Level agreements and Trading Partner Agreements

Service level agreements (SLAs) may be developed for in-house managed and/or developed information resources. Trading partner agreements (TPAs) are often developed for externally managed and/or developed information resources. If SLAs or TPAs are developed, incorporate information security requirements. Information security requirements for securing cardholder data must be incorporated in contracts and memoranda of understanding (MOU) with PCI service providers.

MOUs document the terms and conditions for interagency data and information sharing in a secure manner. An interconnection security agreement (ISA) supports the MOU by specifying the requirements for connecting IT systems and describing the security controls that will be used to protect the systems and data via the certification and accreditation (C&A) process.

8-5.4.6 Register Information Resource in ~~eAccess~~ARIS~~eAccess~~/ARIS

Register the information resource in ~~eAccess~~ARIS~~eAccess~~/ARIS, which is the Postal Service application for managing the authorization process for personnel needing to access the information resource and the associated information. Registration is also required for the use of managed accounts (e.g., machine accounts).

8-5.4.7 Develop Business Continuity and Facility Plans

Business continuity plans must be developed for critical information resources. A facility recovery plan is developed for facilities designated by the vice president Information Technology Operations as major information technology sites. These plans are started during this phase and updated in Phase 5 – System Integration Testing.

8-5.4.8 Identify Connectivity Requirements

Requirements for connectivity to the Postal Service infrastructure must be identified and a request must be submitted to the Network Change Review Board (NCRB) *(see https://usps.service-now.com)*.

8-5.5 Phase 5 — System Integration Testing

The security controls and processes implemented in Phase 4 are tested. The information security activities of Phase 5 are described in the following paragraphs.

8-5.5.1 Develop Security Test Plan

A security test plan must be developed for all information resources. The security test plan evaluates the technical and nontechnical security controls and other safeguards to establish the extent to which the information resource meets the security requirements for its mission and operational environment.

8-5.5.2 Conduct Operational Security Training

Using the training materials developed in the prior phase, users, system administrators, managers, and other personnel are trained on the correct use of the information resource and its security safeguards.

8-5.5.3 Conduct Development of Contingency Plans

The contingency plans (and, if applicable, the facility recovery plan) from Phase 4 – Build must be updated as required.

8-5.6 Phase 6 — Customer Acceptance Testing

Phase 6 consists of activities described below that culminate in the certification, risk mitigation plan, accreditation,

acceptance of residual risk, and approval to deploy an information resource. (See Handbook AS-805-A Exhibit 4-6 for The Certification and Accreditation Input, Activities and Output.)

8-5.6.1 Conduct Security Test and Document Results

Security testing is conducted using the approved security test plan. If a modification to a control is required, the change must be reflected in the security plan and the security test plan before the test is ~~executed. The~~executed. The results of the testing must be documented and communicated in language that is understandable to business-process owners and the ISSO.

(See Handbook AS-805-A Section 4-6.4.2.1 for Conduct The Security Test and Evaluation.)

8-5.6.2 Conduct Security Code Review

To protect the infrastructure, a documented security code review may be required. (See Handbook AS-805-A for the criteria for conducting a code review.)

The security code review is based on the Postal Service Security Code Review Standards or an acceptable equivalent. This security code review is not required if an independent security code review is conducted.

8-5.6.3 Conduct Vulnerability Scan

A vulnerability scan is recommended for all information resources. A quarterly vulnerability scan is required for PCI applications and an annual vulnerability scan is required for externally facing applications. The scanning procedure must ensure adequate scan coverage and the updating of a list of vulnerabilities.

8-5.6.Conduct Risk Assessment

A risk assessment must be conducted for all information resources to identify security concerns (e.g., threats, vulnerabilities, and control weaknesses), risk ranking, additional countermeasures, and residual risk (see 4-3, Information Resource Risk Management). The risk assessment can be started in this phase but must be updated throughout the TSLC.

8-5.6.5 Conduct Independent Risk Assessment

An independent information security risk assessment may be required to evaluate the appropriateness and effectiveness of the security controls and identify residual risk. (See Handbook AS-805-A for the criteria for conducting an independent risk assessment.)

8-5.6.6 Conduct Independent Security Code Review

Information resources may be subject to an independent code review of the source code and documentation to verify compliance with software design documentation and programming standards and the absence of malicious code. The independent code review may also evaluate correctness and

specific security issues. (See Handbook AS-805-A for the criteria for conducting an independent security code review.)

8-5.6.7 Conduct Independent Penetration Testing and Vulnerability Scans

Independent penetration testing evaluates the effectiveness of the implemented information resource configuration. Vulnerability scans evaluate information resources for vulnerabilities and compliance with Postal Service information security policies and standards. (See Handbook AS-805-A for the criteria for conducting independent penetration testing and vulnerability scans.)

8-5.6.8 Conduct Regular Vulnerability Scans

Vulnerability scans evaluate information resources for vulnerabilities and compliance with Postal Service information security policies and standards. (See Handbook AS-805-A for the criteria for conducting independent penetration testing and vulnerability scans.)

8-5.6.9 Perform Penetration Testing

Prior to the first production deployment, or "go live" date, all Postal applications should have penetration testing performed. Operational requirements for penetration testing include ensuring that the system is available for testing, and that penetration testers have access to the application and data nearly identical to a live environment. Objectively, penetration testing should ensure that the application is free of any findings prior to any customer interaction with the application. Postal leaders are responsible for ensuring that enough time is available for the application to be tested.

8-5.6.10 Conduct Independent Validation of Security Testing

The independent security test validation addresses the appropriateness and effectiveness of the security controls and corroborates the previously conducted security test results. The scope of the independent security test validation depends on the information resource, its environment, and the associated threats and vulnerabilities. The independent security test validation is usually carried out at the development or test site. (See Handbook AS-805-A for the criteria for conducting an independent security test validation.)

8-5.6.11 Project Manager and ISSO Develop C&A Documentation Package

Sensitive-enhanced, sensitive, and critical information resources require a C&A documentation package. The project manager and the ISSO develop the C&A package. The package is a consolidation of the designation of sensitivity and criticality and associated protection requirements (BIA); threats, vulnerabilities, additional controls, and residual risks (risk assessment); protection mechanisms (security plan

and business continuity plans); and the security test and evaluation results.

8-5.6.12 Project Manager, Executive Sponsor, and ISSO Prepare Risk Mitigation Plan

The Project Manager, Executive Sponsor, and ISSO prepare a risk mitigation plan for any residual risks rated as medium or high, recommending how the risks will be mitigated, the organization or individual responsible, and the time table for resolution.

8-5.6.13 ISSO Reviews C&A Documentation Package and Prepares Evaluation Report

The ISSO reviews the C&A documentation package and prepares a C&A evaluation report highlighting the findings and recommendations. The ISSO escalates security concerns or forwards the C&A evaluation report and supporting documentation to the certifier for review.

8-5.6.14 Certifier Escalates Security Concerns or Certifies Information Resource

The certifier (e.g., manager, C&A process) reviews the C&A evaluation report and the supporting C&A documentation package, escalates security concerns or prepares and signs a certification letter, and forwards the certification letter and C&A documentation package to the accreditor.

If the certifier decides not to certify the information resource, he or she will indicate the C&A Phase to return to for rework.

8-5.6.15 Accreditor Escalates Security Concerns or Accredits Information Resource

The accreditor (i.e., manager, CISO) reviews the risk mitigation plan and the supporting C&A documentation. Based on this review, the accreditor either, escalates security concerns or prepares and signs an accreditation letter, and forwards the accreditation letter and final C&A documentation package to the vice president functional business area (or the executive sponsor if this responsibility is delegated) and to the vice president of IT (or the Business Relationship Management portfolio manager if this responsibility is delegated).

If the accreditor decides not to accredit the information resource, he or she will indicate the C&A phase to return to for rework.

8-5.7 Phase 7 – Governance and Compliance

No information security activities are associated with this phase.

8-5.8 Phase 8 — Release Management and Production

Phase 7 is the operation and maintenance period of the information resource and includes activities to ensure that chosen security controls and procedures are functioning properly and that security controls are modified or added as needed to continue to protect the information resource. The information security activities for Phase 7 are described in the following paragraphs.

8-5.8.1 Data Conversion

A data conversion plan must be defined so that it incorporates collecting, converting, and verifying data for completeness and integrity and resolving any errors found during conversion. Create a backup of all data prior to conversion and maintain audit trails to track the conversion to ensure there is a fallback and recovery plan in case the conversion fails. Ensure that the backed-up data conforms to the applicable data retention schedule.

8-5.8.2 Deploy Information Resource

~~All three approvals (i.e., certification, accreditation, and approval to deploy) are~~Certification and accreditation approvals are both required before deploying the information resource. When the information resource is deployed, the security controls for the information resource are implemented as documented in the security plan and with the caveats included in the acceptance letter.

8-5.8.3 Information Resource Maintenance

Information resources must be maintained in a timely manner. Critical security patches for PCI-related information resources, including applications and infrastructure, must be installed within 30 days of release. The tools, techniques, and mechanisms used to maintain information resources must be properly controlled.

8-5.8.4 Follow Security-Related Plans and Continually Monitor Operations

The security-related plans must be followed during deployment, operation, and maintenance. The information resource controls must be continually monitored by the project team to ensure they are working as intended and remain in compliance with the security-related plans.

8-5.8.5 Periodically Review, Test, and Audit

Information resources are periodically reviewed, tested, and audited for compliance with Postal Service policies (e.g., plans related to facility recovery or business continuity are tested to ensure that these plans meet business and security objectives).

For non-PCI information resources, a subset of the information security controls must be formally tested annually by the project team, the tests documented, and the results submitted to the applicable ISSO. The security controls that are volatile or critical

to protecting the information system must be assessed at least annually. All other controls must be assessed at least once during the information resource's 3-year accreditation cycle (e.g., one third of these other controls each year).

8-5.8.6 Reassess Risks and Upgrade Security Controls

Risks are re-assessed as part of the re-initiation of the C&A process. Security controls are upgraded as necessary to protect the information resource and assure business continuity.

8-5.8.7 Update Security-Related Plans

Security-related plans are updated in response to changing environment, changing technology, re-assessed risks or vulnerabilities, and as part of the re-initiation of the C&A process.

8-5.8.8 Reinitiate C&A

The criteria for recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process*~~, 6-2.~~.

8-5.8.9 Disposition C&A Documentation

After each information resource has been accredited, zip the electronic versions (PDFs) of the C&A documents and store them in the IT TSLC Artifacts Library for access by the project manager and their project development team. Keep the electronic C&A documents for 4 years after the information resource is accredited.

Keep the hardcopy documents for 1 year after the information resource has been accredited and then destroy in accordance with 3-5.8.

8-5.9 Phase 9 - Retire

8-5.9.1 Dispose of Data

All Postal Service sensitive-enhanced, sensitive, and critical information that is no longer needed, whether in electronic or nonelectronic format, is transferred, archived, or destroyed in accordance with official Postal Service policies and procedures (see 3-5.8, Disposal and Destruction of Information and Media, and Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management).*

8-5.9.2 Sanitize Equipment and Media

All Postal Service sensitive-enhanced, sensitive, and critical information is completely erased or destroyed prior to disposal of the hardware or electronic media on which it resides (see 3-5.8, Disposal and Destruction of Information and Media).

9 Information Security Services

9-1 Policy

Information security services provide the policies, requirements, standards, and processes that enable the integration and implementation of information security across Postal Service information resources to ensure a viable secure computing infrastructure and to protect information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction.

All Postal Service personnel must adhere to the following information security services:

a. Authorization.

b. Accountability.

c. Identification.

d. Authentication.

e. Confidentiality.

f. Integrity.

g. Availability.

h. Security administration.

i. Audit logging.

9-2 Security Services Overview

Information security services provide the framework for implementing information security measures used to protect information resources. Security services are as follows:

a. Authorization determines whether, and to what extent, personnel should have access to specific computer resources.

b. Accountability associates each unique identifier with one user or system process to enable tracking of all actions by the user or of the process on the information resource.

c. Identification associates a user with a unique identifier (i.e., user account or log-on ID) by which that user is held accountable for the actions and events initiated by the identifier.

d. Authentication verifies the claimed identify of an individual, computing device, or originator.

e. Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

f. Integrity ensures the correct operation of information resources, consistency of data structures, and accuracy of stored information.

g. Availability ensures information resources are accessible by authorized personnel or other information resources when required.

h. Security administration implements management constraints, operational procedures, and supplemental controls established to provide adequate protection of an information resource.

i. Audit logging records operational and security-related events.

9-3 Authorization

Authorization provides the framework for determining whether, and to what extent, personnel or on-line users should have access to computer resources. Information resources must be configured to ensure that no user is allowed access to an information resource (e.g., transaction, data, and process) unless authorized by appropriate Postal Service management or approved external user. Upon employment, personnel may be granted access to temporary information services until they receive clearance. External users may need approval to access certain business services. Further details regarding authorization for both internal and external users follow see section 9-3.1

9-3.1 Authorization Principles

Internal Users (workforce):

Access must be granted based on personnel roles and the security principles of clearance, need to know, separation of duties, and least privilege.

External Users (customers):

External User Authorization is the process of giving the user permission to access a specific resource, data set, page/URL or function. Authorization is tied to a business or user service managed by ~~customer registration~~external users. A business or user service translates access authorization to an on-line page/URL, a function, a data set or some other resource. There are a variety of methods used to grant an authorization and a variety of methods used to determine if a user should be authorized to have access to a business service.

a. Methods used to grant an authorization include approval based internal functions and/or external user functions.
b. Internal authorization functions include help desk approval, use of an authorization code (i.e., invitation, promo code or validation code, etc.), identity proofing, credit validation and other Postal Service staff approval methods.

~~a.~~c. External authorization functions include a self-asserted claim by an end user to manage the users associated with a service, a function or function of a company. The first person to make that claim can become the Business Service Administrator (BSA). The BSA then can in turn approve other users to have the same privileges as they do in performing a function or having access to a resource for the same data set. Once a BSA is assigned, external users may then request access to that function or resource. The BSA can either accept the request or deny the request. The BSA can also appoint a delegate who can also make similar approvals. A Delegate approver cannot deny access to a BSA. Some BSA roles are only assigned in coordination with Postal Service personnel to determine the "rightful" owner of that data set or function. Once that BSA is approved by the Postal Service, then the BSA can also add other users to have similar rights.

9-3.1.1 Clearances

For personnel without appropriate clearances or background investigations, access is restricted to temporary information services. Managers must use ~~eAccessARISe~~Access/ARIS to request access authorization for individuals who do not have the appropriate clearance and are responsible for the access activities of those individuals.

9-3.1.2 Need to Know

For sensitive-enhanced, sensitive, and critical information resources access must be limited in a manner that is sufficient to support approved business functions. Access to sensitive-enhanced and sensitive Postal Service information resources must be limited to personnel who need to know the information to perform their duties.

9-3.1.3 Separation of Duties

Only authorized personnel are approved for access to Postal Service information resources. This approval must be specific to an individual's roles and responsibilities in the performance of his or her duties and must specify the type of access (e.g., read, write, delete, and execute); specific resources and information; and time periods for which the approval is valid. Separation of duties and responsibilities are considered when defining roles. For special situations where additional control is required, dual authorization can be implemented.

9-3.1.4 Least Privilege

For sensitive-enhanced, sensitive and critical information resources access is based on providing personnel with the minimum level of information resources and system functionality needed to perform their duties. Systems and applications must define as many levels of access as necessary to prevent misuse of system resources and protect the integrity and confidentiality of Postal Service information. Postal Service information resources must be capable of imposing access control based on specific functions (e.g., create, read, update, delete, and execute).

9-3.2 Authorization Management

~~eAccess~~ARIS~~e~~Access/ARIS is the Postal Service application for managing authorization to information resources. ~~eAccess~~ARIS~~e~~Access/ARIS centralizes the management of personnel and machine identities (i.e., human and nonhuman accounts/identities) and access rights over the entire life cycle, from account creation/registration to termination. ~~eAccess~~ARIS~~e~~Access/ARIS operates on the premise that access is denied unless specifically approved by the user's manager. ~~For many external users, customer registration is the approved application to manage authorization to resources.~~

External Users (customers) – must receive authorization to the approved application for which access is granted. This includes, but is not limited to, Personal User, Business User, Pending and Partial. For authorization requirements, refer to 9-3.3. For a complete description of account management, refer to 9-4.3 through 9-4.3.4.

9-3.2.1 Requesting Authorization

All requests for authorization to access Postal Service information resources, including temporary information services, must be requested via ~~eAccess~~ARIS~~e~~Access/ARIS at ~~*http://eaccessARIS*~~ *https://eaccess.usps.gov*. If access to a Postal information resource cannot be requested through ~~eAccess~~ARIS~~e~~Access/ARIS for any reason associated with a technical limitation of ~~eAccess~~ARIS~~e~~Access/ARIS, then use PS Form 1357.

9-3.2.2 Temporary Information Services

Requests for temporary information services must go through ~~eAccess~~ARIS~~e~~Access/ARIS for proper management approval. For contractor personnel who have submitted their documentation for security clearances or background investigations, the manager, Corporate Information Security Office (CISO), may authorize temporary access to the following information services until the contractor's background investigation is completed and security clearance has been issued:

a. ACE active directory account.

b. E-mail access.

c. Office suite of services.

d. Intranet browser access.

The following information services are unavailable under temporary access: a. Internet browser access.

b. Remote access.

c. Access to e-mail except within the Postal Service intranet.

Note: No access beyond temporary information services will be authorized until the background investigation is completed and the appropriate personnel security clearance is granted. Upon receipt of an appropriate security clearance or background investigation, individuals requiring access beyond temporary information services may request additional authorization via ~~eAccess~~ARIS~~e~~Access/ARIS.

9-3.2.3 Expiration of Temporary Access Authorization

Temporary access expires in 3 months and can be renewed if warranted.

9-3.2.4 Approving Requests

All requests for authorization must be approved by the individual's manager or supervisor, the contracting officer's representative (if the request is for a contractor), and the executive sponsor of the application.

9-3.2.5 Periodic Review of Access Authorization

Managers must review access granted to personnel under their supervision to ensure that the access is still required for personnel to perform their duties. The minimum acceptable review schedule is on a semiannual basis; more frequent reviews should be scheduled based on information sensitivity.

The manager CISO may require that some privileged system/application accounts be reconciled to related ~~eAccessARISe~~Access/ARIS records on a monthly basis. Discrepancies must be investigated and resolved immediately.

9-3.2.6 Implementing Changes

System administrators and database administrators must implement all approved authorization requests for the information resources under their control. They must not add, modify, or revoke access to information resources except in accordance with Postal Service policies.

9-3.2.7 Revoking Access

All managers must ensure that access to information resources is immediately revoked for personnel when no longer required because of a change in job responsibilities, transfer, routine separation or involuntary termination. The immediate manager will advise the system and/or database administrators as to the final disposition of files and data based on the exit date filed by Human Resources.

9-3.2.8 Sudo (Pseudo) Access

Sudo (pseudo) access has higher levels of rights, such as account creation/ update/deletion, full application/platform functionality, or a subset of rights that have been designated as privileged. Sudo access must be restricted to a unique individual whose duties require these additional privileges. Use is restricted to performing those job functions required by the privileged access; individuals must use their regular user accounts to perform non-privileged functions. Applications must not have the capability to run as "root." An audit trail must be maintained on all privileged access.

9-3.2.9 User and Resource Registration Management

User and resource registration management must provide the following functionality to allow managers to perform their roles and responsibilities in the authorization process:

a. Register user or resource to directory service or authoritative source.

b. Assign or furnish unique identifier.

c. Track modifications to user or resource access authorizations.

d. Provide management reports.

e. Validate user or resource identity.

f. Revoke or keep user or resource access (two levels of approvals).

g. Log and audit access requests.

9-3.2.10 Special Account Registration Management

Special account (i.e., Service, Shared and Vendor Default) registration management must be implemented to allow managers to identify special accounts under management control and provide appropriate accountability for the account usage from account creation through termination.

Accounts where access is required to perform credentialed scans are often designated within authentication packages such as ~~eAccessARIS~~eAccess/ARIS as "special" accounts. "Special" accounts must not be used for PCI applications unless (a) required by COTS software to function correctly, (b) the account is properly configured (i.e., treated as an administrator account that will not be used as a true service account), and (c) it does not violate other requirements in this handbook.

All special accounts must be documented, registered, and reviewed by responsible managers (i.e., account custodians) monthly. The responsibilities of an account custodian are as follows:

a. Special accounts are assigned to ~~eAccessARIS~~eAccess/ARIS managers who serve as the account custodians.

b. The custodian is ultimately responsible for the use of these accounts with respect to access of Postal Service information systems.

c. Service accounts (e.g., an account managed by Operating System) must be created with the minimum access rights and privileges required to perform the necessary business function and must be tightly controlled by the account custodian.

d. The account custodian may assign members (including Postal Service employees and contractors) to shared accounts, who should be the sole users of the account. Shared accounts have a single log-on ID that is used by more than one individual. The managed e-mail account may only be created on the usps.gov domain.

e. When a special account is accessible by more than one individual, those individuals (i.e., registered members in ~~eAccessARIS~~eAccess/ARIS) must be registered, approved and reviewed periodically by the account custodian and/or custodian's manager.

9-3.2.11 Emergency Access when Individual is not Available

In instances during which an individual has possession of Postal Service information that is required by his or her manager and the individual is unavailable (e.g., on annual leave), the following process must be followed:

a. The individual's manager initiates a request for access to the information using a documented procedure (e.g., remedy or information ticket). The individual's manager is accountable for the emergency access.

b. Audit logging for all activities related to an emergency access request is required and must be protected and retained according to Postal Service standards.

c. The emergency access must be conducted under the identity of the user authorized by the manager and actually performing the access. Under no

circumstance will the unavailable individual's log-on ID or password be used or compromised in an emergency access.

d. The system administrator either rewrites the access rules giving the manager or the manager's designee access to the information (files), or the system administrator is authorized by the manager to access the information on the manager's behalf.
e. Upon completion of the emergency access, all access to the information is returned to its original state.
f. The unavailable individual is notified of the emergency access as soon as he or she becomes available.

9-3.2.12 Emergency Access to Production Information

In instances during which a developer or database administrator needs emergency (e.g., after hours) access to production information, the following process must be followed:

a. The individual opens a remedy ticket. The individual is accountable for the actions performed during the emergency access.
b. Audit logging for all activities related to an emergency access request is required and must be protected and retained according to Postal Service standards.
c. The emergency access must be conducted under the identity of the individual actually performing the access.
d. Upon completion of the emergency access, all access is returned to its original state.
e. The remedy ticket is closed.

9-3.3 Authorization Requirements

Access to internal ~~Information~~ information resources must comply with authorization requirements including, but not limited to, the following:

a. The information resource must not allow access to resources without invoking the authorization process and checking the assigned rights and privileges of the authenticated user.
b. The information resource must have features to assign user privileges (i.e., access permissions) to log-on IDs, roles, groups, and information resources.
c. Privileges on information resources (e.g., computing devices, consoles, terminals, and subsidiary networks) must not allow the user to bypass or upgrade his or her privileges established in centralized access control lists or databases.
d. The information resource must have the capability to restrict session establishment or information resource access based on time of day, day of the week, calendar date of the login, and source of the connection. Information resources running on operating systems that do not have these capabilities must implement compensating controls (e.g., monitoring devices).
e. The information resource must provide the administrator-configurable capability to limit the number of concurrent log-on sessions for a given user.

f. The information resource must not offer any mechanism to bypass authorization restrictions.

g. Access granted to the information application resource must be accurately reflected in ~~eAccess~~ARISeAccess/ARIS and should not extend beyond the pre-established role definitions.

h. Computing devices, mobile or otherwise, requesting access from remote, non-Postal Service locations must authenticate before access is granted.

External Access compliance instructions are as follows:

a. For information resource accesses that require authorization, the information resource must not allow access to resources without invoking the authorization process and checking the assigned rights and privileges of the authenticated user. Not all information resources require authorization; some only require authentication.
b. The information resource must have features to assign user privileges to User IDs based upon, roles, user services, company records, and related information resources.
c. Privileges on information resources (e.g., data sets, online pages/URLs, functions, etc.) must not allow the user to bypass or upgrade his or her privileges established in centralized customer ~~registration~~ databases.
d. The information resource must have the capability to enable access to external users 24 hours a day, 7 days a week.
e. The information resource must not offer any mechanism to bypass authorization restrictions.
Access granted to the information application resource must be accurately reflected in the customer's ~~registration~~ external account and should not extend beyond the pre-established authorization privileges and definitions.
f. Some form of authentication must proceed authorization approvals.

9-4 Accountability

Accountability is the process of associating any action on the information resource with one and only one user, process, or other information resource and is essential for maintaining minimum levels of information security.

9-4.1 Types of Accountability

Accountability for access to information resources must be established at the site, network, and the individual level.

9-4.1.1 Site Accountability

Site accountability associates users or information resources with a specific location. Site accountability is established by issuing a site identification

number or code (site ID) that is restricted by system hardware or software to a unique system, network, or terminal address in a controlled environment.

9-4.1.2 Network Accountability

Network accountability associates users or information resources with a specific network or logical subnet to a network. Network accountability is established by issuing a network identification number or code (network ID) or through the network address.

9-4.1.3 Individual Accountability

Individual accountability associates each user or information resource (e.g., a workstation or terminal) with any action on an information resource. Individual accountability is established by issuing a unique user or log-on identification number or code (i.e., user ID or log-on ID). Machine accountability may be established for a specific information resource through its workstation address or other identifier. All information resources must be capable of individual accountability and must do the following:

a. Identify information resources each time they attempt to log-on to the system.

b. Verify that information resources are authorized to use the system.

c. Associate all actions taken by an information resource with that resource's unique identifier (i.e., resource ID or log-on ID).

9-4.2 Types of Accounts

Internal users (workforce) – Access to information resources is managed through the use of multiple types of accounts, including the following:

a. User.

b. Privileged.

c. Service.

d. Shared.

e. Vendor default and vendor maintenance.

f. Guest.

Ownership for privileged, shared, and maintenance log-on IDs must be documented and administered in a secured manner.

For a complete description of accounts, refer to 9-4.2.1 through 9-4.2.6.

External users (customers ~~registration~~):

a. Personal User – Used for external users who have a customer ~~registration~~ username and password.

b. Business User – Used for external users (who declared themselves a business user) who have a customer ~~registration~~ username and password.

c. Pending (upgradeable to full account) – Used to track external users who do not have a customer ~~registration~~ username and password but ~~who~~ do have some privileged interaction with a Postal Service information resource.

d. Partial (not upgradeable to full account) – Used to track external users who do not have a customer ~~registration~~ username and password but ~~who~~ do have some privileged interaction with a Postal Service information resource.

9-4.2.1 User Accounts

User accounts provide application/platform users with a minimum level of information resources and application functionality needed to perform their duties (i.e., least privilege) and do not carry special privileges above those required to perform the user's business function. This includes limited access accounts that exist for a specific purpose (e.g., an auditor account).

Application user accounts are used to log into the application via a front-end interface, and the account privileges and roles are restricted by the approved access. Platform user accounts (i.e., database and operating system) are used to access platform-level resources and are limited to non-privileged access rights.

9-4.2.2 Privileged Accounts

Privileged accounts (e.g., administrator or maintenance accounts) are accounts that allow entitled users access to change data, alter configuration settings, run programs, or permits unrestricted access to view data. Assignment must be restricted to a unique individual whose duties require these additional privileges (e.g., system, network, database administrators). Use is restricted to performing those job functions required by the privileged account (e.g., creating new user profiles or altering the rights of existing non-privileged users); individuals must use their regular user accounts to perform non-privileged functions such as Internet access and Postal Service email.

Privileged accounts include Enterprise Admins, Schema Admins, Domain Admins, Administrators, Account Operators, Server Operators, Print Operators, and Backup Operators. Permission inheritance must be disabled for all privileged accounts.

Privileged uses must use two-factor authentication. An audit trail must be maintained on all privileged account usage.

Application accounts must not have the capability to run as "root."

9-4.2.3 Service Accounts

Service accounts are assigned to an information resource (e.g., server, application) or other automated process/service (not an individual) used to process data and/or identify actions or requests. Normally, the operating system uses this account when it hosts a service. Service accounts must be placed under management control. Service accounts must be created with the minimum access rights and privileges required to perform the necessary business function. These accounts must not be allowed root or administrative privileges. They are managed by the Postal Service entity responsible for the life cycle of the account from creation, deployment, usage, and retirement when no longer needed. See 9-6.1.8, Requests for Use of non-expiring Service Accounts for use of service accounts with non-expiring passwords.

9-4.2.4 Shared Accounts

There are two types of shared accounts:

a. Shared accounts (e.g., training accounts) have a single log-on ID and password that is used by more than one individual. A shared account must be used only for qualifying circumstances and when deemed necessary by the CISO. This approach to account usage is highly discouraged and requires the appropriate level of management approval via ~~eAccessARISe~~Access/ARIS as well as approval by the CISO. The use of shared accounts must be tracked (e.g., logged) to manage individual accountability. The requesting manager is responsible for undocumented usage of the shared accounts and is responsible for password management. Shared accounts must not include access to Postal Service production systems, the Internet or the PCI environment. System operators must not share identification or authentication materials of any kind, nor allow any other person to operate any information systems by employing that user's identity. Generic accounts must not be used to administer PCI system components.

b. Managed email accounts are used to provide a single email mailbox that can be shared by multiple users. This mailbox is in addition to their personal regular mailboxes. The account is controlled by the account custodian. The custodian must send an email to the Postal Service Special Account Administrator to request access for a user. "Send As" allows a user to send emails from the name of the mailbox. The password is never shared and each user logs on to his or her workstation with his or her own User ID and password.

9-4.2.5 Supplier and Vendor Default and Maintenance Accounts

Supplier and vendor default accounts are accounts that are pre-installed on a product and must be removed or disabled. Supplier and vendor maintenance accounts are user accounts for the maintenance of their products to resolve issues related to the product and must be enabled only when needed, monitored, and controlled by a responsible Postal Service organization. Supplier and vendor maintenance personnel must not have access (including remote access) to any PCI cardholder data environment or PCI systems without documented business justification and CISO approval.

9-4.2.6 Guest Accounts

Guest accounts are not allowed for access to Postal Service network information resources. Guest accounts expose information resources to risk by allowing access to information resources through the use of a generic logon ID that either uses no password or a widely known password. Guest accounts incorporated into any software or established through any other means must be deleted or disabled. This policy does not apply to guest networks isolated from the Postal Service intranet that are used to support non-Postal Service external access.

9-4.3 Account Management

Internal Accounts (workforce) – Accounts must be established in a manner that ensures access is granted based on clearances, need to know, separation of duties, and least privilege basis. Accounts unused for ~~90~~ 15 calendar days must be disabled.

Accounts unused for 1 year must be deleted. A user account suspension can also be triggered by certain clock rings in Time & Attendance System (TACS)

External users (customers ~~registration~~):

a. Personal User – Used for external users who have a customer ~~registration~~ username and password.

b. Business User – Used for external users (who declared themselves a business user) who have a customer ~~registration~~ username and password.

c. Pending (upgradeable to full account) – Used to track external users who do not have a customer ~~registration~~ username and password but ~~who~~ do have some privileged interaction with a Postal Service information resource.

d. Partial (not upgradeable to full account) – Used to track external users who do not have a customer ~~registration~~ username and password but ~~who~~ do have some privileged interaction with a Postal Service.

~~d.~~e. Personal or business accounts unused for more than 400 days may be disabled. Unused accounts are not deleted. Pending account options to upgrade to a full account ~~in customer registration~~ are only valid for 15 calendar days and then ~~expired~~disabled.

9-4.3.1 Establishing Accounts

Internal Users (workforce):

To establish an account, personnel must request an account from their manager or supervisor via ~~eAccess~~ARISeAccess/ARIS at ~~*http://eaccessARIS*~~ *https://eaccess.usps.gov*.

External Users (customers):

External users may sign up for an external account as needed, and without additional approval by anyone in the Postal Service.

9-4.3.2 Documenting Account Information

Internal accounts (workforce):

The account information, or database, must contain the following information for each user account: log-on ID, group memberships, access control privileges, authentication information, and security-relevant roles. Any security-related attributes that are maintained must be stored securely to protect their confidentiality and integrity.

External accounts (customers):

The account information shall be centrally managed via the customer's ~~registration~~external account. Information about the account must include the following information, Username, User ID, membership details, access controls, levels of assurance, date/time of registration as well as IP address, authentication information and authorization data. Any security

related attributes that are maintained must be stored securely to protect their confidentiality and integrity.

9-4.3.3 Configuring Account Time-Outs

Internal Accounts (workforce)– Accounts must be configured to log the workstation off the network or disable the session after a predetermined period of inactivity and enforce re-authentication. This requirement should be automated where possible. The Postal Service default standard period of inactivity is a maximum of 30 minutes. This action reduces the amount of time Postal Service information resources are vulnerable to compromise. Any deviation from this standard is the responsibility of the executive sponsor and must be documented and approved by the CISO.

External users (customers ~~registration~~) – The session time-out period due to inactivity for external accounts ~~used on customer registration~~ is 15 minutes.

9-4.3.4 Local Accounts

All access to information resources will be through Active Directory accounts/ passwords or Active Directory enforced two-factor authentication protocols. Local accounts are prohibited on all servers, workstations, laptops, and other end-user computing devices (this prohibits the creation of new local accounts and requires the removal of any existing local accounts from the ~~fore mentioned~~ aforementioned resources). Users and operations staff will use individually issued and identifiable Active Directory accounts for access.

Exceptions to this policy are the following:

a. The local built-in administrator account will be retained on all servers, workstations, and laptops but is restricted to operations personnel working on servers or workstations that are disconnected from the network and unable to authenticate to the directory. The local built-in administrator accounts and their passwords will be maintained in accordance with requirements for elevated privileged accounts. These accounts are part of the standard server build/configuration and do not require separate approval or management through ~~eAccessARISe~~Access/ARIS.

b. Mobile computing device access is granted a blanket exception as the current models are restricted to local accounts only. These accounts are part of the standard device build/configuration and do not require separate approval or management through ~~eAccessARISe~~Access/ARIS.

Other exceptions may be granted on case-by-case bases by the CISO and the manager IT Desktop Computing (ITDC) where a COTS product will not work without a local account or there is a compelling business or operational need.

Requests for exceptions to the policy prohibiting local accounts other than the built-in Administrator and mobile computing devices accounts must be made through ~~eAccessARISe~~AccessARIS. The approving manager must be a PCES manager; CISO will be the FSC; and ITDC will be the log administrator. The ~~eAccessARISe~~Access/ARIS system serves as the archive for requests, approvals/denials, and implementation if approved.

9-4.3.5 Departing Personnel

Accounts must be deleted or passwords changed when personnel leave the organization.

9-4.3.6 Vendor Maintenance Accounts

Vendor maintenance accounts must be managed, enabled only when needed by the vendor, and monitored while being used.

9-4.3.7 Handling Compromised Accounts

Internal users (workforce):

Information resources must provide automated mechanisms to support identifying and handling information security incidents. All personnel who suspect an account has been compromised must immediately notify management and follow the incident reporting process (see 13-3.2, Incident Reporting).

External users: (customers ~~registration~~):

All personnel who suspect an account has been compromised must notify eSAFE, ~~customer registration,~~ the Inspection service and the CISO Threat Intelligence Team.

9-5 Identification

~~Internal users:~~

Identification is the process of associating a person or information resource with a unique enterprise wide identifier (e.g., a user log-on ID). The log-on ID is used in conjunction with other security services, such as authentication measures, to track activities and hold users accountable for their actions. Users are responsible for all actions performed on Postal Service information resources under their log-on ID.

Internal users (workforce): Identification requirements for processing and control devices in the mail processing and mail handling equipment (MPE/MHE) environment for private non-routable network address space are defined by Engineering.

External users (customers):

~~External users (customer registration):~~ Online user activity will be tracked based upon a digital identity. Digital identity is the online persona of a subject and is the unique representation of a subject engaged in an online transaction.

9-5.1 Issuing Log-on IDs

Log-on IDs or user IDs are unique groups of letters, numbers, or symbols assigned to a specific person or information resource.

Internal users (workforce): All personnel using Postal Service information resources are issued a log-on ID in conjunction with the authorization process. No two users are assigned the same log-on ID. This policy does not apply to users of managed shared accounts.

External users: (customers ~~registration~~): Users creating an external account ~~in customer registration~~ will be issued a User ID (a number) which will be related to their login or username. No two users are assigned the same log-on ID.

9-5.2 Protecting Log-on IDs

Log-on IDs must be protected in accordance with the following:

a. Personnel must not share their log-on IDs or permit others to use them to access Postal Service information resources.

b. Log-on IDs must not be embedded in application code or batch files or stored in application files or tables unless approved compensating security controls are implemented.

9-5.3 Suspending Log-on IDs

Internal users (workforce) – After six unsuccessful attempts to log on to an information resource, the log-on ID or account must be ~~suspended~~ disabled for a period of at least 5 minutes (or 30 minutes for PCI-related applications or until the system administrator resets the account). If the log-on ID or account does not unsuspend itself after the suspension period, the user must use ePassword Reset or call the Help Desk and follow defined procedures for resolution. ~~Log-on IDs not used within the past 90 days must be disabled and the user must call the Help Desk for resolution.~~

Employees who remain in a Leave Without Pay (LWOP) status for a period in excess of 15 calendar days, or who are expected to be in a LWOP status in excess of 15 calendar days, must have their ~~ARIS~~eAccess/ARIS account ~~suspended~~disabled until such time as they return to an in-work status.

In addition, customers have an option to recover username, if forgotten.

External ~~(customer registration)~~ users (customers) – For externally facing login pages, do as follows,

a. After 5 unsuccessful attempts to log on to a customer's ~~registration~~ managed login page, the user needs to wait 1 minute until they can attempt to login again.

b. With 3 additional unsuccessful attempts, the user will be prompted to wait 5 additional minutes.

c. With 2 additional unsuccessful login attempts (total of 10), the user will be prompted to wait 15 minutes until their next attempt.

d. With 1 additional unsuccessful login attempt (#11), the user will be prompted to wait 30 minutes.

e. With the 12th unsuccessful login attempt, the user will need to wait 1 hour.

f. With the 13th unsuccessful login attempt, the user will need to wait 24 hours until they can login again.

g. For all other customer ~~registration~~-related login pages, after 4 unsuccessful login attempts, the user will not allowed to login again for 24 hours. In both cases (customer ~~registration~~-owned login page and customer ~~registration~~-related login page), customers can also use the I Forgot My Password process to access their account.

~~g.~~

9-5.4 Failed Log-on Attempts

9-5.4.1 Recording Failed Log-on Attempts

Failed log-on attempts must be recorded for audit trail and incident reporting purposes.

9-5.4.2 User Notification of Failed Log-on Attempt

Notification to the user of a failed log-on attempt will reflect only that the logon failed. The reason for the failed log-on attempt and information previously entered, including the disguised or clear password, must not be returned to the user.

9-5.5 Terminating Log-on IDs

Internal users (workforce) ~~– Inactive~~ Log-on IDs not used for the last 365 days must be deleted.

External users (customers) – Log-on IDs not used in the last 365 days must be deleted.

External ~~(customer registration)~~ users (customers) – External accounts are not deleted for non-use.

9-5.6 Identification Requirements

Internal users (workforce) :

Information resources must comply with security requirements including, but not limited to, the following:

a. The information resource must, at a minimum, use log-on IDs as the primary means of identification.

b. The information resource must have the capability to automatically disable a log-on ID that has not been used for an administrator configurable period of time.

c. The information resource must not allow an administrator to create, intentionally or inadvertently, a log-on ID that already exists.

d. A log-on ID must not exist without associated authentication information.

e. The information resource must not provide any process to bypass the authentication information for any log-on ID.

f. The information resource must have the capability of associating each internal process with the log-on ID of the user who initiated the process. Processes that are not initiated by a user, such as print spoolers, database management servers and any spawned sub-processes, must be associated with an identifier code, such as "system ownership."

External users (customers ~~registration~~):

a. The information resource must, at a minimum, use User IDs as the primary means of identification of a user's account.
b. The information resource must have the capability to disable an account that has not been used for an administrator-configurable period of time.
c. The information resource must not allow an administrator to create, intentionally or inadvertently, a unique account that already exists.
d. A User ID can exist without associated authentication information.
e. The information resource must not provide any process to bypass the authentication information for any log-on ID.
~~a.~~f. The information resource must have the capability of associating each on-line activity with the User ID of the user who initiated the process.

9-6 Authentication

Internal Users (workforce): Authentication is the process of verifying the claimed identity of an individual, workstation, or originator. While identification is accomplished through a logon ID, authentication is achieved when the user provides the correct password, personal identification number (PIN), or other authenticator associated with that identifier. Internal users or ~~P~~personnel must be required to identify and authenticate themselves to the information resource before being allowed to perform any other actions.

External users (customers):

Digital authentication establishes that a subject/claimant attempting to access a digital service is in control of the technologies used to authenticate. This approach supports privacy protection by mitigating risks of unauthorized access to individual's information. Authentication of a user's account may occur via username/password, or via username in conjunction with shared secrets or via synchronized access tokens. Location and device identity are not considered authentication factors.

Access to any database containing cardholder data must be authenticated. This includes access by applications, systems and database administrators, and users. Direct access and queries to PCI databases must restricted to database administrators and must be logged.

Authentication requirements for processing and control devices in the MPE/ MHE private non-routable network address space are defined by Engineering.

Means of authentication, or authenticators, may include the following:

a. Passwords.

b. Personal identification numbers.

c. Shared secrets.

d. Digital certificates and signatures.

e. Smart cards and tokens.

f. Biometrics.

g. Strong authentication.

9-6.1 Passwords

Passwords are unique strings of characters that personnel or information resources provide in conjunction with a log-on ID to gain access to an information resource. Passwords, which are the first line of defense for the protection of Postal Service information resources, must be treated as sensitive information and must not be disclosed.

9-6.1.1 Password Selection Requirements

Password requirements must comply with the following:

Internal application users (workforce): – Password requirements must comply with the following:

a. For all users, passwords for all platforms except mobile devices must consist of at least 15 characters and contain at least one character from three of the four following types of characters: English uppercase letters (A–Z), English lowercase letters (a–z), Westernized Arabic numerals (0–9), and nonalphanumeric characters (i.e., special characters such as &, #, and $).

b. Password requirements associated mobile devices will be based on the capability of the hardware and software and can be found in the appropriate policy/procedure documents.

c. The only nonalphanumeric characters available for the mainframe are: @, #, and $.

d. For all users, passwords must not contain the user's name or any part of the user's full name.

e. Passwords must not be repeated (reused) for at least five generations.

External application users (~~users of~~ customer~~s~~ ~~registration~~; *www.usps.com*, Business Customer Gateway, and related applications) – Password requirements must comply with the following:

a. Passwords must consist of at least 8 characters and contain at least one upper case character (A-Z), one lower case character (a-z), and one number (0-9). Special characters are allowed but are limited to the following: – ().&@?',/"+!).

b. The password must not contain more than 2 consecutive repeat characters.

c. Passwords cannot match the username.

9-6.1.2 Password Selection Recommendations

The following password recommendations are prudent security practices intended to enhance the password complexity and protect the password from attempted password cracking:

a. Do not use family member names or other information easily discovered about the user (e.g., license plate number, phone number, birth date, and street name).

b. Do not use commonly used words such as words that appear in the dictionary or Postal Service terminology.

c. Do not use all the same characters or digits or other commonly used or easily guessed formats.

d. Use longer password conventions whenever possible (e.g., passphrases and run-on multiword strings).

e. Do not use all the same characters or digits or other commonly used or easily guessed formats, such as: a1a1a1a1 or 123d123d.

f. To remember your passwords and make them stronger, instead of thinking in terms of pass 'words', think in terms of '~~phases~~phrases', where your password is a short phrase separated by special characters or numbers. Examples would be: Kick_the_can1; 4Jump-the-shark4; and Ocean5Sunset.

g. Use industry best practices (such as banking, FICAM) to determine allowable passwords.

9-6.1.3 Initial Password

Internal users (workforce): – Passwords must always be delivered in a secure manner. The initial password for users must be sent via protected electronic delivery system or personal delivery to the user (First Class Mail is also acceptable). For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at log-on.

Note: Caution must be taken not to use standard~~ize on~~ generic or global passwords when issuing new accounts or when resetting forgotten passwords.

9-6.1.4 Password Suspension

Internal users (workforce) – After six unsuccessful attempts to log on to an information resource, the log-on ID or account must be ~~suspended~~ disabled for a period of at least 5 minutes for internal systems accessed via ACE and non-ACE devices, (or 30 minutes for PCI-related applications or until the system administrator resets the account).

External users (customer~~s registration~~) – For externally facing login pages:

a. After 5 unsuccessful attempts to log on to a customer ~~registration~~ managed login page, the user needs to wait 1 minute until they can attempt to login again.

b. With 3 additional unsuccessful attempts, the user will be prompted to wait 5 additional minutes.

c. With 2 additional unsuccessful login attempts (total of 10), the user will be prompted to wait 15 minutes until their next attempt.
d. With 1 additional unsuccessful login attempt (#11), the user will be prompted to wait 30 minutes.
e. With the 12th unsuccessful login attempt, the user will need to wait 1 hour; with the 13th unsuccessful login attempt, the user will need to wait 24 hours until they can login again.
f. For all other customer ~~registration~~-related login pages, after 4 unsuccessful login attempts, the user will not be allowed to login again for 24 hours.
g. In both cases (customer ~~registration~~-owned login page and customer ~~registration~~-related login page), customers can also use the I Forgot My Password process to access their account.

9-6.1.5 Reset Passwords

Internal users (workforce)– Users with non-privileged accounts who have forgotten their passwords or need to perform routine password resets, should reset their password by invoking ePassword Reset. The exception to using the ePassword Reset system is for privileged, machine and vendor default accounts (see below). The ePassword Reset system requires user authentication prior to allowing the user to perform a password reset. If a user calls the Help Desk to reset a password, users are challenged by Help Desk personnel to provide further confirmation of identity prior to resetting the password. Password change requests via the Help Desk are documented via a change request ticket. The password is reset to a temporary password by an administrative group, and the user must then change the password at first log-on.

ePassword Reset is not used for privileged, machine, and vendor default accounts. The passwords to these accounts are changed by the system administrator group via the Help Desk. When users of these accounts request the reset of a password, the users are challenged by Help Desk personnel to provide further confirmation of their identity (e.g., some predetermined shared secret that only the user would know) prior to resetting the password. Upon confirmation of user identity, the request is documented via a change request ticket and assigned to the appropriate administrator group for resetting the password. For privileged accounts, the administrator group resets to a temporary password and the privileged user must then change the password at first log-on.

External users (customer~~s registration~~) – For ~~Customer Registration~~external users, passwords may be reset as follows:

a. Help-desk call. Users calling the help desk are challenged by helpdesk personnel to provide further confirmation of their identity prior to resetting the password. Upon confirmation of the user identity, the request is documented in the ~~customer registration~~external users internal application. A temporary password can be sent by the help-desk personnel via email to the end user. Upon receipt, the user can type in their username and temporary password. Users will then need to enter a password into ~~customer registration~~external users application to complete their login.

b. I Forgot My Password self-service process. External customers may reset their passwords via entering the answers to their secret questions into ~~a customer registration~~the external users page. If successful, the user will then be prompted to type in their new password to complete their login.

c. SMS Account Recovery. Customers who have signed up for account recovery via SMS codes can enter the code received by verification text or email on the webpage.

9-6.1.6 Password Expiration

Internal users (workforce)– The information resource must offer an authentication information-aging feature that requires users to periodically change authentication information, such as passwords. All Postal Service personnel must change their passwords when prompted by the system or risk being locked out, thus requiring assistance to reset the account. Password expiration requirements are as follows:

a. Prior to the expiration of authentication information, such as passwords, the information resource provides notification to the user.

b. At least every 30 days, passwords for privileged accounts or for those accounts considered sensitive (e.g., system supervisors, software specialists, system administrators, database administrators [DBA, SYSDBA, SYSOPER, INSERT ANY TABLE, UPDATE ANY TABLE, DELETE ANY TABLE], or vendor-supplied) must be changed.

c. At least every 90 days, passwords for all other accounts must be aged and changed.

Oracle database schema accounts are assigned to a database (not an individual) and are typically considered the application owner. These accounts have minimum access rights and privileges required to perform the necessary business functions with respect to the application. Oracle Database Schema Accounts closely resemble Service Accounts as they are not granted root or administrative privileges and are placed under management control [Database Systems and Services (DBSS) is the Postal Service entity responsible for the life cycle of the account from creation, deployment, usage, and retirement when no longer needed]. DBSS is responsible for password maintenance on all Oracle Database Schema Accounts. DBSS must take the following measures to protect the password:

a. The password is not provided to anyone outside of DBSS.
b. If the password is stored in a database, it is encrypted.
c. If the password is stored in a file, the file is protected.
d. If scripts need to be run as the schema account, DBSS staff enters the password.
e. The password for schema accounts must comply with a password strength function that enforces the password to be at least 15 characters long. This is necessary because the schema account password does not expire so extra measures are taken to protect it.
f. DBSS has monitoring in place on all databases for usage of this account and records all suspicious activity.

External users (customers ~~registration~~) – There are no requirements for external customers to change their passwords on a periodic basis.

9-6.1.7 Requests for Use of Nonexpiring Password Accounts

All requests for use of nonexpiring password accounts must be approved by the manager, CISO. The manager CISO must be added as a FSC for all machine accounts. These accounts are tracked for compliance purposes. The executive sponsor is accountable for the use of these accounts. If approval is granted, the following compensating controls must be implemented:

a. Account must be in a centrally managed database. No privileged access allowed.

b. Encrypt the LDAP call to keep the password from being transmitted across the network in clear text.

c. Change password when personnel with access to the account leave or transfer.

d. Non-expiring password accounts must be requested and documented through ~~eAccess~~ARISeAccess/ARIS.

e. Ownership of non-expiring password accounts must be identified and recertified on a semi-annual basis.

f. Rights and privileges of non-expiring password accounts must be reviewed at least on a semi-annual basis to evaluate the appropriateness of access.

g. Passwords for non-expiring password accounts must use a complex password that exceeds standard length requirements.

h. Source-restrict the account to a specific host and do not allow console or remote entry.

i. Restrict access to the password to operations staff with a need to know.

9-6.1.8 Requests for Use of Non-expiring Service Accounts

All requests for use of non-expiring password service accounts must be submitted in writing (e-mail is acceptable) by the executive sponsor to the manager, CISO. The rationale for these accounts is to prevent service interruptions due to a locked account. These accounts must be tracked for compliance purposes. The executive sponsor will be held accountable for the implementation of these accounts. If approval is granted, the following compensating controls must be implemented:

a. Account must be requested and documented in ~~eAccess~~ARISeAccess/ARIS.

b. No privileged access allowed; specific ACL's must be applied under the concept of 'least privilege'. Use of root, system administration, non-cancel, etc. privileges are prohibited.

c. Account must not have the rights to modify or delete system (e.g., syslog or Windows System Event) or security log files.

d. Restrict account's usage to a specific host.

e. Direct login to the service account, whether from a console or remote session, is prohibited and must be disabled.

f. Rights and privileges of account must be reviewed and validated on a semi-annual basis.

g. Non-expiring password must meet Postal Service standards, including password length and complexity, and be encrypted in storage and in transit. The only exceptions to the criteria are password aging and account suspension on failed login attempts.

h. Restrict access to password to operations staff with a need to know and change when personnel with access leave or transfer. Comply with 6-6, Departing Personnel, to terminate all access when personnel leave or are transferred.

9-6.1.9 Password Protection

Passwords used to connect to Postal Service information resources must be treated as sensitive information and not be disclosed to anyone other than the authorized user, including system administrators and technical support staff. Requirements for protecting passwords include the following:

a. Passwords must not be shared except those used for shared accounts.

b. If passwords are written down and stored outside the user's personal control, they must be secured in a tamper-resistant manner (e.g., an envelope with registry seal, time stamped, and signed by the user) to ensure that any disclosure or removal of the written password is clearly recognizable.

c. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user or has been otherwise compromised, the user must immediately change the password and notify CyberSafe.

d. Passwords must be encrypted in transit.

9-6.1.10 Password Storage

Passwords must be stored in one-way encrypted format where possible. There may be cases where business requirements for the system are unable to meet one-way encryption implementation, these exceptions should be identified and documented as part of the certification and accreditation process. Passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems must be encrypted using the Postal Service encryption standard documented in 9-7.1.1, Minimum Encryption Standards, and decrypted when used.

Passwords for ~~customer registration~~ external users may not be decrypted when used.

9-6.1.11 Vendor Default Passwords

Vendor-supplied default accounts must be disabled, removed, or the passwords must be changed before connecting the system or introducing the software to the Postal Service network. This includes passwords used by contractors or consultants when configuring a system.

9-6.1.12 Password Requirements

Internal users (workforce) – Information resources must support the following password requirements:

a. Deny access if the user does not comply with password selection or expiration criteria.

b. Set initial password to a temporary password and require user to change the temporary password on first log-on.

c. Suspend account after an administrator-configurable number of unsuccessful entries.

d. Require re-authentication by the user, as well as reconfirmation of the new password, at the time of an attempted password change.

e. Mask password entry during the authentication process.

f. Store passwords in a one-way encrypted format.

g. Encrypt passwords in transmissions.

h. Require users to change passwords (password aging every 90 days or when compromise is suspected).

i. Change vendor-supplied default passwords prior to use.

External users (customers ~~registration~~):

Information resources must support the following password requirements:

a. Accept user created passwords that only comply with the password selection criteria.

b. Lock account after an administrator-configurable number of unsuccessful entries.

c. Require reconfirmation of the new password at the time of an attempted password change.

d. During the password entry process, allow one letter/character to be shown to the user as they type in the password and mask the previous entry after each subsequent password character is entered.

e. Store passwords in a one-way encrypted format.

f. Encrypt passwords in transmissions via HTTPS/POST.

g. Do not require users to change passwords on a periodic basis.

h. Enable a forced change to user passwords based upon a data breach or known fraudulent activities.

9-6.2 Personal Identification Numbers

PINs are a specialized type of authenticator that are used in conjunction with unique identifiers to verify the identity of users before allowing them access to information resources. Use Postal Service 4-digit PINs only for limited interfaces such as the Integrated Voice Response (IVR) based non-sensitive applications. Do not use Postal Service 4-digit PINs for Human Resource self-service web-based applications.

Where technologically capable, use of PINs with increased complexity are mandatory in order to meet challenges posed by increasing information

security threats and developing technological advancements. Where technically capable, these PINs must include the following composite design: eight-character minimum combination of numbers, letters, and special characters, with a defined window for expiration.

Like passwords, PINs must be treated as sensitive information and must not be disclosed. All personnel must comply with Postal Service policies regarding PIN management and usage and are directly responsible for all actions taken using an assigned identifier and PIN.

9-6.2.1 PIN Generation and Selection Requirements

To ensure that PINs retain integrity and confidentiality, PINs must be protected during generation and dissemination. All personnel are encouraged to change their PIN from the initial assignment. PINs must:

a. Be a minimum of four characters in length, two of which are unique.

b. Avoid obvious combinations or sequences.

c. Avoid well-known or easily guessed combinations (e.g., social security number, telephone number, and house address).

9-6.2.2 PIN Distribution

Secure delivery methods include First Class Mail, an encrypted delivery system, or personal delivery to the user. New or replacement PINs must not be delivered by telephone, facsimile, or electronic mail to protect against unauthorized disclosure.

9-6.2.3 PIN Protection

PINs must be committed to memory or stored in a secure location. Information resources must store PIN data in an encrypted format that meets Postal Service encryption standards. All access, additions, modifications, and deletions to the PIN data must be logged and monitored. If PIN authentication is performed over an open network, such as the Internet, PINs must be encrypted during transmission according to Postal Service encryption standards.

9-6.2.4 Forgotten PINs

When requesting replacement of a forgotten PIN, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes. All forgotten PINs must be replaced with securely delivered new PINs.

9-6.2.5 Suspension

When using a PIN for authentication, the information resource must be disconnected after three incorrect entries and the PIN account suspended after six incorrect entries. When a suspended PIN account is reactivated, the user must be assigned a new PIN that is delivered via secure methods.

9-6.2.6 PIN Cancellation and Destruction

A PIN suspected of compromise must be cancelled immediately and a new PIN generated and delivered via secure methods. Unauthorized users who no longer require access to the system must be removed immediately. All PIN data must be destroyed when the user no longer requires access to the system or leaves Postal Service employment.

9-6.2.7 PINs Used for Financial Transactions

PINs used for financial transactions must comply with American National Standards Institute Financial Services Technical Publication X9.8, PIN Management and Security. Financial transactions at high risk for fraud may not be suitable for reliance on PINs as the primary authentication mechanism.

9-6.3 Shared Secrets

A shared secret is an authentication mechanism used to re–set a user's password or PIN. When requesting the reset of a password or PIN, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes.

Internal users (workforce)– shared secrets must comply with the following:

a. Be a minimum of eight characters.

b. Be protected and stored as sensitive information.

c. Be stored encrypted if stored electronically.

d. Have the user's account ~~suspended~~ disabled if the shared secret is entered incorrectly three times.

e. Ensure an information resource using shared secrets provides a secure process for recording an initial shared secret and changing the shared secret in the event of suspected compromise.

External users (customers ~~registration~~):

a. Be a minimum of three characters.

b. Be protected and stored as sensitive information.

c. Be stored encrypted if stored electronically.

d. Do not allow changes to shared secrets.

9-6.4 Digital Certificates and Signatures

A digital certificate is an X.509 certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer, or service identity contained within the certificate. The certificate's purpose is to relate a unique name to a specific public key and is used for encryption and decryption of files and the nonrepudiation of messages. USPS sets standards for the properties, utilization, and acceptance of digital certificates in USPS systems and applications where digital certificates are used.

Cryptographically, X.509 is the standard defined by the public key certificate within USPS. As defined in 11-1.1.4, the Postal Service uses X.509 certificates for secure communication, including the TLS and SSL protocols. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual). When signed by a trusted certificate authority, someone holding that certificate can rely on the public key it contains to authenticate the identity presented therein.

An X.509 is defined by the International Telecommunications Union's Standardization sector (ITU-T), and is based on ASN.1, another ITU-T

standard and contains information about the identity to which a certificate is issued and the identity that issued it. Standard information in an X.509 certificate includes the following:

a. Version – which X.509 version applies to the certificate (which indicates what data the certificate must include).

b. Serial number – the identity creating the certificate must assign it a serial number that distinguishes it from other certificates.

c. Algorithm information – the algorithm used by the issuer to sign the certificate.

d. Issuer distinguished name – the name of the entity issuing the certificate (usually a certificate authority).

e. Validity period of the certificate – start/end date and time.

f. Subject distinguished name – the name of the identity the certificate is issued to.

g. Subject public key information – the public key associated with the identity.

h. Extensions (optional).

Within the Postal Service, the CISO determines the eligibility of each proposed role, group, code signer, system, application, or device to receive one or more certificates. The CISO determines and verifies the identity of the human sponsor for each proposed role, group, code signer, system, application, or device to receive one or more certificates

9-6.4.1 Digital Certificate

A digital certificate contains a public key and a private key. Digital certificates are used for identity verification prior to performing a separate action [by way of another process entirely, such as the Transport Layer Security (TLS) protocol] to transmit data securely. The Postal Service sets 9-6.4.2

standards for the properties, utilization, and acceptance of digital certificates in Postal Service systems and applications where digital certificates are used.

A public key certificate is a digitally signed document that serves to validate the sender's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (which may be either a user or a system name) and the holder's public key, as well as the digital signature of a certification authority for authentication. The certification authority attests that the sender's name is the one associated with the public key in the document. A user ID packet, containing the sender's unique identifier, is sent after the certificate packet. There are different types of public key certificates for different functions such as the following:

Device:

a. Web server SSL.

b. IPSEC tunneling.

c. Active directory authentication.

d. Data servers.

e. Secure terminal services.

f. Code signing.

g. Secure LDAP.

User:

a. PIV identification cards.

b. Client authentication.

c. Document signing and encryption.

d. Secure E-mail.

e. Encrypted file system (EFS).

9-6.4.2 Digital Signature

A digital signature is a digital code that can be attached to an electronically transmitted message or file that uniquely identifies the sender. The signature is used to authorize action, to demonstrate responsibility, and legally to indicate intent of decisions. Digital signatures enable electronic approvals promoting business efficiencies. Digital certificates are required when using digital signatures. Digital signatures perform three important functions:

a. Integrity allows the recipient of a given message or file to detect whether that message or file has been modified.
b. Authentication makes it possible to verify cryptographically the identity of the person who signed a given message.
c. Nonrepudiation prevents the sender of a message from later claiming that they did not send the message.

9-6.4.3 Certificate and Signature Standards

Certificate Authority (CA) operating requirements are defined within this policy, and may also be well-defined within a Certificate Policy (CP) document. This includes digital certificate properties, as well as utilization and acceptance. Certificate Authority server operational practices are defined within the Security Plan document for each Enterprise Information Repository (EIR) at the Postal Service that operates the Certificate Authority (CA) servers, and may also be well-defined within Certificate Practice Statement (CPS) documents. If used, CPS documents are required for each CA Server and are used to describe how each of those CA servers are operated in accordance with the relevant CP document under which they must function.

9-6.4.4 Digitized Signatures

A digitized signature is a handwritten signature reproduced in its identical form as a TrueType font or graphical image. The signature may be embedded in electronic messages or documents as a representation of an individual's signature. There are no security associations with a digitized signature, e.g., non-repudiation and document integrity.

9-6.4.5 Certificate Stores

A Certificate Trust Store is a permanent storage where a Public Key Infrastructure (PKI) stores its certificates, CRLs, and certificate trust lists. A trusted root certificate is the cornerstone and trust anchor of authentication and security on the Internet.

Vendors' products come pre-populated with many root certificates in their trust stores, potentially certificates that Postal Service does not want to implicitly trust. The CISO sets the direction of what should be included in the trust stores and the Public Key Infrastructure Management Authority (PKIMA) provide technical assistance to application and system owners with regards to the content of installed product's trust stores through automated or manual processes, to include the following:

a. Removing all certificates that have passed their expiration date.

b. Removing all certificates that are no longer trusted.

c. Removing all certificates that are no longer required..

9-6.4.6 Naming Constraints

Names for certificate issuers and certificate subjects are of the X.500 Distinguished Name (DN) form. The "United States Postal Service" is a registered name in accordance with American National Standards Institute. The U.S. National Name Registration Authority uses of this identifier within USPS are not restrictive because the identifier is unambiguous and may be used in a variety of environments and various encoding methods. To be unambiguous, USPS must establish context and naming hierarchies. A single naming hierarchy is established within the Postal Service as outlined below:

a. Names for certificate issuers (i.e., USPS CA) and certificate subjects (i.e., subscriber or end entity) are of the X.500 DN form. These names are unique and unambiguous within the USPS hierarchy.
b. Certificate issuers have entries at the organization name level. The DNs follow the following form: OU=United States Postal Service, O=U.S. Government, C=US.
c. Certificate subjects have entries at the organizational Unit Name level. The DNs must follow the following form: CN=Subscriber Name, OU=United States Postal Service, O=U.S. Government, C=US.

Certificate subjects choose an optional Alternated Subject Name if marked noncritical. Certificate subjects choose to have additional name forms, such as an e-mail address; however, the DN is the primary name and the one used to populate the subject fields of certificates and CRLs. Additional objects outside the scope of this policy must also be present in the naming hierarchy.

9-6.4.7 Meaningful Names

All names, including machine names and application names, are unique and understandable to humans. The DN must represent the subscriber in a way that is easily interpretable. For people, this is a legal name. For equipment, this is a model name and serial number. Distinguished names must be unique for all end entities of the USPS CA. X.500 DNs are used, and the USPS CAs enforce name uniqueness within the X.500 name space for which they have been authorized. When name forms other than a DN (e.g., e-mail address or DNS name) are used, they too are allocated to ensure name uniqueness.

The contents of each certificate Subject and Issuer name field have an association with the authenticated name of the Entity. A certificate issued for a device or application must include, within the Directory entry, the name of

the person or organization responsible for that device or application. All certificates have name constraints asserted that limit the name space of the CAs to that appropriate for the domain.

9-6.4.8 Rules for Constructing Various Name Forms

Name forms are contained in the applicable certificate profile. As the USPS organization responsible for management and operation of the USPS X.500 directory. The Information Technology Engineering and Architecture (ITEA) group is responsible for the USPS X.500 directory name space and works with the Change Management Process for naming approval prior to final certificate provisioning.

9-6.4.9 Name Claim Dispute Resolution Procedure

Any dispute related to a name claim between USPS and an organization or individual outside of USPS is resolved using the following dispute settlement mechanism:

a. A dispute is resolved by negotiation if possible.

b. A dispute not settled by negotiation is resolved through arbitration by the USPS PKIPA.

9-6.5 Smart Cards and Tokens

Smart cards and tokens are tangible objects that usually contain a built-in microprocessor to store and process information used to verify the identity of a user. Smart cards and tokens are valid methods of authentication. The CISO must approve all implementations of these technologies for accessing information resources. The CISO, in conjunction with the Inspection Service, sets standards for the use and protection of smart cards and tokens. All personnel must protect smart cards and tokens from theft and not allow others to use them.

9-6.6 Biometrics

Using biometric information is a valid method of authentication. Biometrics are technologies used to authenticate individuals by means of unchanging biological characteristics (e.g., fingerprints, palm prints, voice prints, or facial, iris, and retina scans). The CISO must approve all implementations of biometric technologies for accessing information resources. Biometric information is sensitive-enhanced information and must be protected. The CISO, in conjunction with the Inspection Service, sets standards for the use of biometric authentication and the storage of biometric information.

9-6.7 Strong Authentication

Strong authentication consists of two-factor or multifactor authentication tools (e.g., smart card and PIN or thumbprint and password) that move toward the concept of nonrepudiation or conclusive tracing of an action to an individual. Single-factor authentication tools such as log-on IDs and passwords do not provide strong authentication.

Strong authentication is required for external native apps that are downloaded via an APP Store, such as Google PlayStore or ITunes. Native apps will encrypt the payload. Native apps will use two factor authentication

to establish an encrypted channel through which payloads are communicated.

9-6.8 Nonrepudiation

Nonrepudiation is the security property that ensures that the sender cannot deny sending the message, the recipient cannot deny receiving the message, and actions can be conclusively traced to a specific individual. When required, an information resource must have the capability to support nonrepudiation.

A single public/private key pair and its associated certificate issued to any device may be used for signing (including authentication), key management (for encryption), or both. Device certificates must not assert nonrepudiation as well; all subscriber private keys must not be used by more than one entity.

9-6.9 Remote-Access Authentication

Postal Service information resources must support and maintain access control for personnel using networked, and Internet connections to Postal Service information resources. Strong authentication or other stringent access controls must be implemented for personnel entering through the Internet, or other non-Postal Service communication networks. Source restrictions (i.e., destination verification of remote session source address) may be used as a substitution to strong authentication for remote access. Two-factor authentication is required for remote access to PCI cardholder data.

Multifactor authentication is required for remote access to sensitive, sensitive-enhanced, and PCI cardholder data. Application owners centrally manage all remote access connections to their systems and ensure that remote access capabilities provide strong multi-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. All remote access connections must support cryptographic based, multifactor authentication. Any multifactor authentication is based on USPS-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions must comply with the encryption requirements of FIPS 140-2, Level 3, and Security Requirements for Cryptographic Modules.

9-6.10 Session Management

A computer session is a unique period of activity performed on or by an information resource usually associated with a login by a user. All information resources must implement session management standards specific for the information resource platform.

9-6.10.1 Session Establishment

Internal users (workforce)– Information resources must comply with session establishment requirements including, but not limited to, the following:

a. During a login, the information resource must allow the entire login sequence to be completed before providing any response to the initiator of the login.

b. The information resource must generate an alarm after an administrator-configurable number of consecutive incorrect login attempts across multiple accounts.

c. When the threshold for invalid consecutive attempts (normally six) for a given log-on ID is reached, the information resource must deactivate access for the log-on ID for a period of at least 5 minutes (or 30 minutes for PCI-related applications or until the system administrator resets the account).

d. Upon successful session establishment, the information resource must make available the date and time of the last successful login.

External ~~(customer registration)~~ users(customers):

a. During a login, the information resource must allow the entire login sequence to be completed before providing any response to the initiator of the login.

b. The information resource must generate an alarm after an administrator-configurable number of consecutive incorrect login attempts across multiple accounts.

For externally facing login pages:

a. After 5 unsuccessful attempts to log on to a customer ~~registration~~ managed login page, the user needs to wait 1 minute until they can attempt to login again.

b. With 3 additional unsuccessful attempts, the user will be prompted to wait 5 additional minutes.

c. With 2 additional unsuccessful login attempts (total of 10), the user will be prompted to wait 15 minutes until their next attempt.

d. With 1 additional unsuccessful login attempt (#11), the user will be prompted to wait 30 minutes.

e. With the 12th unsuccessful login attempt, the user will need to wait 1 hour; with the 13th unsuccessful login attempt, the user will need to wait 24 hours until they can login again.

f. For all other customer ~~registration~~-related login pages, after 4 unsuccessful login attempts, the user will not allowed to login again for 24 hours.

g. In both cases (customer ~~registration~~-owned login page and customer ~~registration~~-related login page), customers can also use the I Forgot My Password process to access their account.

Upon successful session establishment, the information resource must make available the date and time of the last successful login.

9-6.10.2 Session Expiration

Information resources must comply with session expiration requirements including, but not limited to, the following:

a. After the specified period of inactivity during the session (applicable standards defined by the manager, CISO ISS), the information resource must terminate the session and connection and require a successful re-authentication to regain access.

b. Following termination by the user or interruption by a power failure, system crash, or transmission problems, the session and connection must be dropped. The establishment of a new session requires the normal user identification, authentication, and authorization.

c. The information resource must provide an administrator-configurable session expiration (i.e., session lifetime). After the specified period of time, regardless of activity, the information resource must terminate the session, lock out the connection, and require a successful re-authentication to regain access.

9-6.10.3 Time-Out Requirements (Re-authentication)

The inactivity time-out standard for Postal Service information resources is a maximum of 30 minutes with the following exceptions:

a. For end-user devices and consoles associated with PCI applications, servers, and network devices the maximum is 15 minutes.

b. For conference rooms used for presentations the maximum is 2 hours.

c. For executives at the vice president level or higher the maximum is 2 hours.

d. For external end users (associated with a customer ~~registration~~ login), the maximum is 15 minutes.

After the maximum of period of inactivity, the information resource must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password. Any deviation from these requirements must be approved by the manager CISO and the executive vice president/CIO.

Manual re-authentication must be required before access to the information resource is re-established. For remote access, the session must be terminated and the information resource disconnected from the network.

Note: Use the Postal Service standard or refer to the specific platform configuration standards for the applicable time-out requirements.

9-6.10.3.1 End User Computing Devices

Internal users (workforce) – After the maximum period of 30 minutes of inactivity, the time-out event must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password. Manual re-authentication must be required before access to the end user computing device is reestablished.

External ~~(customer registration)~~ users (customers) – After the maximum period of 30 minutes of inactivity, the user will be required to log-in again to re-establish a new session. The establishment of a new session requires the normal user identification, authentication, and authorization.

9-6.10.3.2 Applications

After the maximum of period of inactivity define above, the application must time-out.

9-6.10.3.3 Remote Access

For remote access, the communications session is limited to 2 hours. After 2 hours, the end user computing device is asked to re-authenticate to the network. The normal end user computing device inactivity time-out standard described above applies.

9-6.10.3.4 **Failed Access Attempts**

Failed access attempts and access attempts by unauthorized personnel or information resources must be rejected and recorded for audit trail and incident reporting purposes.

9-6.11 Single Sign-On

Single sign-on (SSO) is the automated authentication for additional systems after the user has logged on once. The authenticating system passes the user information to the subsequently called system. This is done in the background; that is, the user does not need to authenticate himself or herself again after his or her first log-on. Certificate-based, two-factor authentication is required to ensure the identity of users accessing the sensitive information within SSO environments. All SSO initiatives must be implemented according to the architectural plan to ensure seamless integration within the enterprise and to avoid the establishment of isolated, unsupported islands.

9-6.12 Authentication Requirements

All information resources must comply with authentication requirements including, but not limited to, the following:

a. The authentication process should protect the information resource from a replay attack.

b. During information resource recovery, authentication information must be recoverable without unauthorized disclosure or loss of data and information resource integrity.

c. The information resource must support a configuration capability that prevents authentication information (e.g., password, PIN number, token, or smart card) from being displayed in clear text or otherwise made available to any other user, including an administrator.

d. When the initial authenticator is created, the information resource must not divulge the authenticator to anyone other than the user and the authorized administrator.

e. The information resource should have the ability to authenticate itself to the user and to other software application components during the authentication sequence.

f. Where technically feasible, information resources must support process-to-process authentication.

g. Failed log-on attempts must be recorded for audit trail and incident reporting purposes.

9-7 Confidentiality

Confidentiality is the security property that ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Information resources must have the capability to ensure that information is transmitted and stored in a way such that only authorized users are allowed access. Confidentiality is maintained through comprehensive and interrelated efforts that include, but are not limited to, the following: a. Information designation.

b. Clearances and need to know.

c. Physical security.

d. Authentication of users.

e. Encryption.

9-7.1 Encryption

Encryption is the primary means for providing confidentiality services for information that can be stored or sent over the network, intranet, and Internet. Information resources that store, process, or transmit sensitive-enhanced or sensitive information must have the capability to encrypt information.

9-7.1.1 Minimum Encryption Standards

Synchronous encryption: Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/ retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.

Asynchronous encryption: RSA with a 2048-bit encryption key pair. Elliptic curve algorithms ECDH or ECDSA may be used with key sizes 224-bit or greater. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.

PCI systems also require Transport Layer Security (TLS) protocol version 1.2. New implementations must meet the minimum standard. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.

The minimum encryption standard for the Postal Service is the Advanced Encryption Standard (AES) with a 256-bit encryption key. ~~PCI systems also require Transport Layer Security (TLS) protocol version 1.1 or higher, but 1.2 is recommended. New implementations must meet the minimum standard. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.~~ Asynchronous encryption: RSA with a 2048-bit encryption key pair.

9-7.1.2 Required for Transmission and Storage

Information resources storing, processing, or transmitting sensitive-enhanced or sensitive information must implement encryption based on Postal Service encryption and key recovery policies. Encryption must be used for sensitive-enhanced and sensitive information that is transmitted across networks or in transit between [1] an application or batch server and a database server and [2] between workstations and a database server.

Encryption must be used for sensitive-enhanced and sensitive information stored or archived on fixed and removable devices or media (e.g., disks, diskettes, CDs, and USB storage devices).

Encryption must also be used for sensitive-enhanced and sensitive information that is stored off Postal Service premises.

Encryption must be used for non-publicly available electronic information in transit or stored off Postal Service premises.

Encryption must be used for payment card industry (PCI) information throughout the life cycle. Unencrypted primary account numbers (PANs) must not be sent via end user messaging technologies.

9-7.1.3 Recommended for Storage on Postal Service Servers and Mainframes

Where technically feasible, encrypt sensitive-enhanced and sensitive information stored on Postal Service non-removable devices.

9-7.1.4 Required for Workstations and Laptops

Full disk encryption must be installed on all workstations and laptops.

9-7.2 Use of Encryption Products

Encryption products must comply with requirements including, but not limited to, the following:

a. Information resources using encryption must use only algorithms and standard encryption products that are approved by the Postal Service and meet federal information processing standards and industry best practices. Use of locally generated, self-signed digital certificates is prohibited.

b. All encryption products must support functionality of and integrate with security content-filtering applications or make encryption keys available to management. Any use of encryption without such technology must be approved in writing by the CISO.

c. Application owners follow encryption standard operating procedures for their application as documented within their specific EIR deliverables, as required by USPS Handbook AS-805-A (4-4.2 Deliverables, a. Standard operating procedures).

9-7.3 Key Management

Key management is the generation, recording, transcription, distribution, installation, storage, changing, disposition, and control of cryptographic keys. Key management must be rigorous and disciplined because attacks against

encryption keys are far more likely to occur and succeed than attacks against encryption algorithms.

9-7.3.1 Protecting Encryption Keys

Encryption keys must be treated as sensitive-enhanced information and access to those keys must be restricted on a need to know basis. The following principles apply to the protection and access of encryption keys:

a. If keying material is generated and stored, the information resource must provide secure key storage that is resistant to compromise through a logical or physical attack.
b. If hardware-based key generation and storage is used, the key must be stored in such a way that it cannot be retrieved in clear text.

9-7.3.2 Recommended Key Management Practices

The best way to mitigate the risk of keys being attacked is to store them in hardware on a secure physical device. Postal Service information resources should adhere to key management procedures and practices that include, but are not limited to, the following:

a. Generate strong keys that meet the Postal Service minimum encryption standards (See 9-7.1.1, Minimum Encryption Standards).
b. Key management should be fully automated and not require manual steps.
c. Generate and store all keys in hardware.
d. Never remove keys from the hardware and never store them in the host's memory.
e. Gain access to the hardware only through a trusted path.

9-7.3.3 Key Management Requirements

Information resources must comply with key management requirements including, but not limited to, the following:

a. If the information resource supports key recovery, then access to the key must be restricted to authorized personnel.
b. The information resource must have the capability to enforce the immediate revocation of user accounts and the associated key(s).
c. Encryption keys must not appear in clear text outside a cryptographic device.
d. Split knowledge keys must be implemented.
e. Dual control of keys must be established.
f. Secure key distribution and storage must be implemented.
g. Unauthorized substitution of keys must be prevented.
h. Keys must be changed periodically, as defined below:
   (1) Every year for PCI in-scope applications.
   (2) Every 2 years for non-PCI in-scope applications.
   (3) Every 3 years for USPS Certificate Authority (CA) Online Subordinate tier Server(s), every 5 years for Offline Policy tier CA server(s), and every 10 years for offline Root tier CA server(s).

(4) Whenever anyone with knowledge of a portion of a key that is NOT stored in a Hardware Security Module (HSM) changes positions, transfers, or for any reason leaves the employ of the Postal Service (e.g., resigns, retires, terminates).

i. Known or suspected compromised keys must be replaced.

j. Old or invalid keys must be revoked.

k. Old keys must be archived and destroyed as applicable.

l. Key custodians must sign a form stating they understand and accept their key-custodian responsibilities.

m. Keys must not be sent in the same email as the encrypted file.

n. Sponsors for nonhuman subscribers (systems, applications, and devices) are responsible for the security of and use of the subscriber's private keys.

o. All subscribers including human and device private keys are not used by more than one entity.

p. Public keys (Digital Certificates) must be changed at least 30-days prior to the digital certificate's expiration date.

9-7.3.4 Public and Private Key Management Agreement

The United States Postal Service (USPS) Cryptographic Keys (aka Private Keys) and Digital Certificates (aka Public Keys); including those provided by third-party vendors intended for use by the USPS, must be used only in accordance with this Public and Private Key Management Agreement, including the following:

a. To use your Cryptographic Key(s) and Digital Certificate(s) exclusively for authorized management of a USPS asset, or authorized USPS business partner asset.

b. To take all necessary precautions to protect your Cryptographic Key(s) and Digital Certificate(s) from loss, disclosure, modification, or unauthorized use, as per this policy derivative; as well as USPS Handbook AS-805C, *Information Security for General Users.*

Every United States Postal employee and contractor shall maintain control of Cryptographic Keys at all times and shall abide by the agreements above.

9-7.4 Cryptographic Hash Function

A cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, hash value, such that an (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest. The ideal cryptographic hash function must have the following significant properties:

a. It is easy to compute the hash value for any given message.

b. It is infeasible to generate a message that has a given hash.

c. It is infeasible to modify a message without changing the hash.

d. It is infeasible to find two different messages with the same hash.

The Postal Service cryptographic hash standard is SHA-2 or SHA 256. Older algorithms (e.g., SHA 1) maintained by commercial products and applications

used and developed by the Postal Service may continue to be supported since they may be required to validate digital signatures executed in the past and to decrypt objects encrypted in the past using the older algorithms and key sizes. These cases must show acceptable effort of migration to standard algorithms as identified in this policy and receive an exception waiver by the CISO. In addition it is recommended that:

a. A Salt value is always used with your hash. This is especially important if the sensitive data to be protected is short like a ~~password~~, social security number, or a payment card number.

b. Always use a Strong Salt value when creating a credential hash. A Salt is a fixed-length cryptographically-strong random value. Follow these practices to properly implement credential-specific salts:

   (1) Generate a unique salt upon creation of each stored credential (not only per user or system-wide).

   (2) Use cryptographically-strong random data.

   (3) As storage permits, use a 32-byte or 64-byte salt.

c. The Salt value should be protected as any other cryptographic value.

9-7.5 Elimination of Residual Data

The information resource must have the capability to ensure that there is no residual data exposed to unauthorized users.

9-8 Integrity

Integrity is the security property that ensures correct operation of information resources, consistency of data structures, and accuracy of stored information. Information resources must be installed and maintained in a manner that ensures the integrity of the information resources and their data.

Appropriate planning must occur before conducting security-related activities affecting the information resource in order to minimize the impact on the integrity of the information resource and on Postal Service operations (e.g., mission, functions, image, and reputation) and assets. Security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, testing, exercises, and retirement and disposal of hardware and media.

9-8.1 Information Resource Integrity

Information resource integrity ensures that information resources perform their intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Integrity provides assurance that under all conditions the operating hardware and software maintain logical correctness, reliability, and effective protection mechanisms. Acceptable integrity thresholds for processing and control devices in the MPE/MHE private non-routable network address space are defined by Engineering. Information resources must comply with information resource integrity requirements including, but not limited to, the following:

a. Security features designated in approved hardening standards must be invoked.

b. No information resource may undermine the integrity of underlying platforms or supporting infrastructure.

c. The information resource must perform integrity checks for system functions.

d. The information resource must retain the existing security parameters even after a restart or recovery.

e. Backup capability must be provided to restore the information resource to its former state.

f. Boundary checking must be implemented to prevent buffer overflow conditions.

g. The information resource must provide appropriate alert messages before executing potentially damaging commands.

h. The information resource must provide an administrator with the capability of retrieving the date and time associated with any security-related activity and the log-on ID of the user who initiated the activity.

i. The information resource must provide mechanisms to detect duplicate authentic financial transactions.

j. The information resource must monitor the status of its components in real time to ensure that all components are still active and to prevent components from failing without detection.

9-8.2 Data Integrity Requirements

Data integrity is the security property that ensures that data meets a given expectation of quality and has not been exposed to accidental or malicious modification or destruction. All input data must be appropriately validated. Information resources must comply with data integrity requirements including, but not limited to, the following:

a. Information resources must have the capability to ensure that data is not modified, altered, or deleted without authorization in either storage or in transit.

b. Any unauthorized modification of data must yield an auditable security-related event.

c. The information resource must have the capability of identifying the originator of any information before that information is used in any restricted function of the information resource.

d. The information resource must log any attempt by the administrator to authorize any user to bypass the administrator-configured data integrity controls.

e. The information resource must protect data integrity by performing data integrity checks.

f. When data integrity checks fail, the information resource must reject the data.

9-8.3 Application Requirements

Management must be made aware of the accuracy, timeliness, and relevance of the information they use for decision making. Management

must be notified if controls which ensure the integrity of information fail or if such controls are suspected of failing.

If information issued or released has been modified in any way, the recipients must be notified about the nature of the modification so that they can determine whether the modifications are significant enough to affect decision making. All incomplete or obsolete information must be suppressed and not distributed to users unless it is accompanied by an explanation which describes the status of the information.

Production data and software must be changed only by authorized people according to established written procedures. Production transactions must be properly authorized prior to updating production records whether these records are computer based or not.

To facilitate tracking and problem resolution, each accountable transaction must be time stamped, identified to person who submitted it, and assigned a unique sequence number or identifier. Line numbering must also be implemented for free-form text messages that deal with important business matters.

Sufficient controls must be implemented to ensure information is free from a significant risk of undetected alteration.

All rejected input transactions must be placed in a suspense file and listed in exception reports until such times as they are successfully resubmitted for processing or otherwise handled. All input transactions that are held in a suspense status pending further investigation must be either resubmitted or otherwise handled within 10 business days of original entry. Input transactions that are corrected for resubmission or that are suspended and later approved resubmission must be subjected to the same validation procedures (e.g., reasonable checks and formal edit checks) that original input transactions receive.

9-8.4 Management Requirements

Internal records must be reviewed semiannually for reasonableness and accuracy. Reasonable checks include ratio analysis and accuracy checks include physical inventories. If records are discovered to be in error, they must be immediately corrected by authorized individuals using standard control procedures.

Important information on which management depends must be compared semiannually with external sources or otherwise cross-validated to verify that it is accurate.

9-8.5 End-User Computing Requirements

End-user computing, including spreadsheets and other user-developed programs, must be documented and regularly reviewed for processing integrity, including their ability to sort, summarize, and report accurately. For important reports, the logic should be reviewed semiannually to verify information is processed completely and accurately. User-developed systems must be secured from unauthorized use. Audit logs must be reviewed daily to detect unauthorized access attempts and take corrective action. To facilitate audit trail requirements, transactions affecting sensitive-enhanced, sensitive, and critical information must be initiated only by receipt of source documents

or computerized messages in which the originating individual and system are clearly identified. Proof of non-Postal Service sources can be achieved via digital signatures, message authentication codes (MACs), and encryption. All end-user business-related representations must be truthful at all times.

9-9 Availability

Availability is the security property that ensures information resources are accessible by authorized personnel or information resources when required.

9-9.1 Capacity Planning and Scalability

For all information resources, capacity planning and scalability must be considered for both the information resources and network components, such as routers, firewalls, proxies, and encryption. Whenever technically feasible, consider scalable information resources that require little or no change to the configuration or the application when adding hardware or data storage.

9-9.2 Redundancy

Redundant systems for utilities, communications, mainframes, servers, and firewalls may be recommended where warranted to ensure the availability of critical information resources. The implementation of redundant systems should be based on a cost-benefit analysis and the recovery time objective (RTO). Infrastructure including telecommunication services must be engineered to not have a common point of failure.

9-9.3 Relationship of Criticality, Recovery-Time Objective, and Recovery-Point Objective

9-9.3.1 Criticality

The initial determination of criticality of an information resource is determined during the BIA process. Subsequently, internal and external dependencies must be identified to understand how a given application interfaces with the rest of the Postal Service applications and infrastructure. A system is dependent if it cannot function without the input or connection to the other system or portal. For example, applications which by themselves are not critical may have a higher designation because they provide data to an application with a higher criticality designation. Any identified dependencies may change the initial criticality designation.

The criticality determination may be further refined by Postal Service management. The criticality designation will be updated in the BIA and EIR by the Business Continuity Group.

9-9.3.2 Recovery-Time Objective

The RTO, which is the maximum allowable downtime for an information resource, is determined for information resource designated as critical. The

RTO is the length of time it takes to restore the information resource. The RTO does not indicate how much data will be lost.

The RTO must be commensurate with the level of criticality. If there is a significant mismatch between the RTO and the criticality designation, the RTO and criticality designation must be reviewed. As a general rule the more critical the information resource, the lower the RTO. A lower RTO often requires a larger investment in BCM resources, which, in turn, results in higher costs. The RTO is determined in consultation with the DR service provider as the DR strategy is defined.

9-9.3.3 Recovery-Point Objective

Also at this time, the data currency requirements/recovery point objective (RPO) is determined. The RPO indicates the maximum amount of allowable data loss. It is the point in time (age) to which data must be recovered relative to the time of the disaster. It is the size of the window of opportunity for data loss. The amount of data loss is determined by backup methods and frequency of backup transport offsite.

9-9.4 Assuring Availability

Multiple technologies should be used to minimize the data loss and increase the availability of data for local and alternate site recovery. These technologies must provide for both traditional backup and recovery to meet local requirements in addition to the availability of data at the alternate processing site for disaster recovery. The movement of data for disaster recovery can be moved electronically over high-speed dedicated circuits via hardware data replication, remote tape vaulting, or information resource specific database replication/journaling technologies. The choice of technologies is dependent on the desired RPO and RTO.

9-9.4.1 Data Replication

Selection criteria: The files selected for data replication are determined by the placement of the data on the appropriate storage device that is configured for passive replication. Passive replication refers to a process when the data is changed and stored on the primary device and then the data is replicated to a device at the alternate site.

Frequency: The frequency of data replication should be aligned for minimal data loss and expected RPO for this service.

9-9.4.2 Remote Tape Vaulting

Selection criteria: The files selected for remote tape vaulting are determined by the usage of unique identifier(s) in the file name or specific request to the IT operations group. The supporting IT operations group needs to be contacted to receive the appropriate unique identifiers or to make specific site requests.

Frequency: The frequency of tape vaulting is dependent on the establish RPO for this service.

Inventory: An inventory of critical files that are remotely vaulted must be maintained. A copy of the inventory must be available at the alternate processing site to support business resumption process.

9-9.4.3 Application Database Replication and Journaling

The application owner who chooses to use a vendor-provided database replication and journaling services for high-availability services must procure the IT-approved product, then fund or perform the necessary configurations and reconfigurations.

9-9.4.4 Alternate Backup Requirements

All information resources not using one of the above technologies must implement secure backups. The information resource must have the capability to check the integrity of data read from a backup file when performing a restore function.

All essential components of an information resource required for continued operations must be backed up. The backup procedures must be documented. The responsible Postal Service manager must define the appropriate backup media and frequency.

Applications determined by the BIA as critical must implement backup and recovery strategies sufficient to meet the RTO and data currency requirements.

9-9.4.4.1 What to Back Up

Backups include, but are not limited to, operating systems, configuration files, general utilities, application software, data, supporting files and tables, scripts, standard operating procedures, specialized equipment, and related documentation.

9-9.4.4.2 When to Back Up

Backup software prior to migrating to test or production and prior to maintenance. Backup software after migrating to production and after maintenance. Backup information updated by batch processing at the successful completion of the update. Backup information updated by real-time processes at a frequency based on the RTO and RPO of the application.

9-9.4.4.3 Backup Schedules

All essential components must be backed up on a schedule that is sufficient to meet the RTO and RPO of the application or information resource as defined by the executive sponsor that controls the essential component and Business Continuance Management. Back-up job failures are properly documented, investigated, and remediated immediately.

9-9.4.4.4 Backup Inventory

An inventory of critical applications backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off site or in a fireproof container at the facility that hosts the application. An inventory of backup media and materials is recommended for all other information resources.

9-9.4.4.5 Backup Storage Requirements

Backup media containing critical information must be stored in an environmentally controlled and secure location (e.g., a locked cabinet or room with controlled access). Backup media containing sensitive-enhance, sensitive, and non-publicly available information must be labeled as

"Restricted Information". Backups must not be stored on the same hardware device as the original information.

9-9.4.4.6 Off-Site Backup Storage Requirements

Critical information stored on mainframes, servers, workstations, and mobile devices must be backed up and must be stored off-site at a location that is not subject to the same threats as the original media. An inventory listing of backup media containing critical information must be maintained at a designated Postal Service facility off site from the primary information location.

Noncritical information stored on mainframes, servers, workstations, and mobile devices must be backed up and stored off site at a location that is not subject to the same threats as the original information. Postal Service information must not be co-mingled with non-Postal Service information.

9-9.4.4.7 Backup Verification

Backup media for critical applications must be verified to ensure that backups are complete and can be read. From time to time, the application and associated backup hardware and software should be tested with the backup media to ensure the application can be successfully restored and used. Verification of backup media is recommended for all other information resources.

Annually review the data backup policies and inspect the actual backup practices of third party providers.

9-9.4.4.8 Backup Disposal

All unneeded electronic backup media or hardware containing sensitive-enhanced or sensitive electronic media must be erased using a method that complies with the most current Postal Service policy and processes on the disposal of sensitive-enhanced and sensitive media. (See 3-5.8, Disposal and Destruction of Information and Media.)

9-9.5 Information Resource Recovery and Reconstitution

Critical information resources, including infrastructure and applications, must have the ability to be recovered and reconstituted to their original state following a disruption, failure, or disaster. This means all system parameters (either default or established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application software is reinstalled, information from the most recent backups is available, and the entire configuration has been fully and successfully tested at an alternate site. Authorization to request backup data is limited and restricted to approved Postal Service personnel.

Contingency plans must be developed and tested for critical infrastructure and telecommunication service providers and include recovery and reconstitution of critical applications. The EIR must be updated to identify which applications require the development and testing of continuity plans.

The frequency for testing business continuity plans for critical-moderate and critical-high applications is defined in 12-2. Business continuity plans for critical-high applications must be tested at an offsite location using only software, data, scripts, and procedures stored at the offsite backup location. The business continuity plans must be updated annually based on the lessons learned from testing.

9-9.6 High Availability

High availability should be implemented where warranted, based on a cost benefit analysis and RTO. Resources or processes that may be deployed to ensure high availability include, but are not limited to, the following: a. Fault-tolerant information resources.

b. Redundant hard drives (e.g., randomly accessed independent disk [RAID] array), systems, and servers.

c. Uninterruptible power supplies (UPS), power conditioning systems, and backup generators.

d. Off-site vaulting of application transactions.

e. Disk mirroring of applications at site not subject to the same threats. Disk mirroring does not negate the need for backups. Mirroring only ensures both instances are the same (i.e., both instances can be blank or incorrect).

f. Hot-swappable components.

g. Secondary storage devices.

h. Continuous monitoring.

i. Automated fail-over and fail-back systems.

9-10 Security Administration

Security administration includes management constraints, operational procedures, and supplemental controls established to protect information resources. Sensitive-enhanced, sensitive, and critical information resources must implement logical access security.

9-10.1 Security Administration Requirements

Security administration functions that must be implemented for Postal Service information resources include, but are not limited to, the following:

a. Activating protective features (e.g., the login feature).

b. Displaying users logged on.

c. Creating, retrieving, updating, or deleting all security–related attributes of users, interfaces, and software and data elements.

d. Overriding or altering vendor-provided security defaults.

e. Configuring security-relevant options.

f. Configuring the display of security-related events.

g. Recording and archiving the information resource configurations.

h. Monitoring suspected activities related to a potential information security incident.

i. Detecting information security incidents immediately, isolating and investigating the problem, and recovering securely from the incident.

j. Provide a level of access and documentation necessary to perform comprehensive security assessments of an information system, application, or hardware when performing the following functions:

1. Incident Response
2. Investigations of Cyber Risk
3. Penetration Testing

9-10.2 Security Administration Documentation Requirements

Security administrative requirements must be appropriately documented. These security administration documentation requirements include, but are not limited to, the following:

a. Cautions about functions and privileges that must be controlled when running a secure facility.

b. Administrator functions related to security, including adding or deleting users, changing user security characteristics, generating keying material, and revoking user-related security parameters.

c. Standards on consistent and effective use of security features, including their interaction and how to generate a new security configuration.

d. Standards for retaining accountability tracking information for an administrator-specified period of time.

e. Procedures necessary to start the information resource in a secure manner.

f. Procedures to resume secure operation after termination of information resource processes.

9-11 Audit Logging

All information resources must implement system-level audit logging. Audit logs include operating system logs, application system logs, database system logs, event logs, error logs, and Web logs. CISO must have access to all security-related audit logs. Information resources must support audit log capabilities including, but not limited to, independently and selectively monitoring (in real time) the following:

a. The actions of any user currently logged on and automatic lockout of that user if necessary.
b. The activities at a specified terminal, port, or network address and automatic lockout of that input device if necessary.

9-11.1 Audit Logging Functionality Requirements

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred. Information resources must implement audit logging functions including, but not limited to, the following:

a. Providing adequate information for establishing audit trails relating to information security incidents (as part of forensics analysis) and user activity.
b. Where feasible, consolidate audit records from all sources for automated analysis, alerting, and archiving in support of compliance, accountability, and security.
c. Supporting administrator-selectable alerts for specified security- related events.
d. Recording the log-on ID or user ID accountable for the event.
e. Maintaining the confidentiality of authenticators (e.g., passwords) by excluding them from being recorded.
f. Maintaining the confidentiality of personally identifiable information (PII) and debit/cardholder data.
g. Protecting audit logs as sensitive information.
h. Protecting audit log control mechanisms from modification, deletion, or disabling of the function.
i. Restricting access to authorized users.
j. Generating real-time alarms indicating immediate attention is required for operational problems (e.g., running out of storage space) and audit log malfunctions. USPS Authorizing Official(s) (AOs) ensure that reports on information security operations status and incident reporting are provided to the policy authority as required by this policy.
k. Providing authorized individuals with access to enable retrieval, printing, and archiving (copying to long-term storage devices) of audit log contents.
l. Providing administrators with audit analysis tools to selectively retrieve records from the audit log to produce reports.
m. Sanitizing audit log storage locations and media prior to reuse.

9-11.2 Audit Log Events

The logging of the following events must be considered for information resources:

a. All sessions established.
b. All authentication attempts (i.e., valid/authorized and invalid/ unauthorized) to access information resources.

c. Action of individuals with root or elevated privileges (e.g., system and database administrators).

d. Creation or changes in user or information resource security accounts, profiles, ACLs, privileges, and attributes.

e. Creation and deletion of system level objects.

f. Use of privileged accounts.

g. Shutdowns, restarts, and backups.

h. Installation and updates of software.

i. Access to audit logs.

j. Changes to log configurations.

k. User Access to Cardholder data.

For the specific security events to capture for a particular platform, see the appropriate hardening standards.

9-11.3 Audit-Log Contents

The information resource must record event information including, but not limited to, the following when available:

a. Date and time of the event.

b. Log-on ID and MAC or IP address of the event initiator.

c. Event type and success or failure of the event if applicable.

d. Identification of information resources accessed.

e. Source host name and IP address generating the log event.

f. Destination host name and IP address generating the log event.

g. Transaction code or process ID.

9-11.4 Audit-Log Protection

Secure audit logs so they cannot be altered by:

a. Labeling audit logs as "RESTRICTED INFORMATION."

b. Limiting the viewing of logs to those with job-related need (e.g., need to know and least privilege).

c. Protecting audit log files from unauthorized access, modifications, and destruction.

d. Immediately backing up audit log files to a centralized server or media that is difficult to alter.

e. Storing a backup copy of audit logs off site.

f. Using file integrity monitoring and change detection software on logs to ensure existing log data cannot be changed without generating alerts.

9-11.5 Audit-Log Reviews

System administrators and database administrators must review audit logs regularly for potential security incidents and security breaches and maintain a record of the review. System administrators and database administrators

must review audit logs regularly for potential security incidents and security breaches and maintain a record of the review. For PCI in-scope applications, audit logs must be reviewed daily. Any suspicious activity must be reported to management and CyberSafe, investigated, documented, and resolved immediately. See Audit-Log Events for details regarding the events that should be captured for each platform.

9-11.6 Audit-Log Retention

Audit logs, whether in electronic or nonelectronic format, must be retained in accordance with a legal hold (e.g., FOIA request, subpoena, law enforcement actions), or as directed by the Postal Service Records Office (see Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management)* and then destroyed in accordance with Postal Service policy.

For PCI in-scope applications, audit logs must be retained for at least one year with a minimum of 3 months immediately available for analysis; (i.e., processes must be in place to restore at least the last three months of logs for immediate analysis).

Industry audit log retention best practice is 2 years online and federal government audit log retention best practice is 18 months online.

10 Hardware and Software Security

10-1 Policy

Postal Service policy is to manage the procurement, configuration, operations, and maintenance of information resource hardware and software, whether located on Postal Service or non-Postal Service premises, in a manner that ensures information security. Hardware and software security must be implemented and maintained with the appropriate level of technical and administrative controls to protect the Postal Service technology and operations infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction. Chapter 10 addresses the following:

a. Hardware security.
b. Software and applications security.
c. General policies for hardware and software.
d. Configuration and change management.
e. Protection against viruses and malicious code.
f. Operating system, database management system, and application audit log requirements.

10-2 Hardware Security

Hardware security must be implemented based on Postal Service published standards on all computer hardware including, but not limited to, the following:

a. Mainframes.
b. Network devices.
c. Servers.
d. Workstations.
e. Mobile computing devices.

10-2.1 Mainframes

Appropriate security controls must be enabled. For mainframe implementation of this security policy, contact the manager, Host Computing Services.

10-2.2 Network Devices

Appropriate security controls must be enabled on all network devices, including servers, routers, hubs, and switches (see 11-3, Protecting the Network Infrastructure).

10-2.3 Servers

A server is a host that provides one or more services for other hosts over a network as a primary function. Servers include outward-facing publicly accessible servers (such as Web and email services); inward-facing servers (such as storage-based information resources like file servers, Network Attached Storage [NAS] servers, Storage Area Network [SAN] servers, database servers, application servers, directory servers, domain name servers); highly specialized servers like security infrastructure devices (such as firewalls and intrusion detection systems); and virtual servers.

Postal Service servers must be protected commensurate with the level of sensitivity and criticality of the information and business function. Server installation and deployment must comply with standard configuration and deployment standards unique to the individual server platform. Implement only one primary function per server [e.g., a Web server, database server, and domain name server (DNS) should be implemented on separate servers).

The following security activities are required to securely administer Postal Service servers:

a. Harden server and configure operating system to address security.

b. Identify vulnerabilities and install additional mitigating controls as required.

c. Implement Postal Service change control procedures.

   (1) Apply and test non-critical patches in a timely manner.

   (2) Implement critical security patches according to Postal Service standards.

   (3) Implement a management process over script automation that includes documentation and inventory of automated scripts.

d. Control automated time synchronization (also see 11-2, Network Infrastructure).

   (1) Implement Network Time Protocol (NTP) or similar technology for time synchronization.

   (2) Designate specific external hosts (i.e., industry-accepted time sources) from which the designated Postal Service time servers will accept NTP time updates.

   (3) Implement controls to prevent internal servers from receiving time signals from any source other than the Postal Service-designated internal NTP servers.

   (4) Restrict access to time data to individuals with a need to access time data.

   (5) Log, monitor, and review all changes to time settings.

e. Determine the best authentication credentials for each operating environment.

f. Implement access control.

   (1) Implement the Postal Service access control policy.

(2) Monitor password aging. Passwords associated with devices that do not have the ability to monitor password aging for local accounts must be submitted for approval as non-expiring passwords.

(3) Conduct semiannual review of all access.

g. Only accept connections from remote clients configured to Postal Service standards.

h. Implement Postal Service standards for audit logging (see 9-11, Audit Logging).

(1) Analyze log files on a frequent basis.

(2) Retain log files according to the applicable system of record.

i. With the application owner determine if server is production or non- production and the server's criticality.

j. Back up critical information and all server software frequently and send backups offsite in accordance with Postal Service processes.

k. Develop appropriate contingency plans and procedures.

l. Establish and follow procedures for recovering from compromise.

m. Implement the following security principles:

(1) Fail safe – fail in a secure manner; (i.e., default to no access).

(2) Separation of privilege – provide a much granularity as possible.

(3) Least privilege – grant minimum rights to perform a task.

(4) Psychological acceptability – implement sensible options that are user acceptable and effective.

(5) Least common mechanism – grant a function to a single process or service.

(6) Defense in depth – implement layered security mechanisms.

(7) Work factor – the amount of work necessary for an attacker to break the system or network should exceed the value of the data or resource availability that the attacker would gain.

(8) Compromise recording – logs provide sufficient evidence if a compromise does occur.

n. Test security controls periodically.

o. Conduct vulnerability scans and penetration tests.

Configuration standards for servers in the mail processing and mail handling equipment (MPE/MHE) non-routable address space environment are defined by Engineering.

10-2.3.1 Hardening Servers

All information resources must be implemented on servers hardened to Postal Service standards. Hardening standards are based on CIS sources and vendor recommendations which must be implemented specific to each platform. These standards must delineate restricted and prohibited functions, port, protocols, and services and include details on how to configure systems with approved security parameter settings.

Server hardening standards must require the removal of unnecessary functionality such as drivers, scripts, subsystems, and file systems.

Hardening standards must be updated as new vulnerabilities are uncovered and updates are available. Hardening standards must be reviewed and updated at least annually. This requirement includes hardening standards for mainframes, servers, networks, and firewalls.

Operating system and database software configurations, including services, protocols and functionality, must be reviewed on a periodic basis commensurate with the level of sensitivity and criticality of the information and business function. Operating system software configuration reviews are performed on a semi-annual basis for UNIX. Unnecessary services and protocols must be disabled. All unnecessary functionality such as scripts, drivers, features, subsystems, and file systems must be removed. Vendor supplied default passwords must be removed and common parameters must be set to prevent misuse or compromise.

Servers must not be deployed to a production environment prior to hardening. Servers must be updated when the server hardening standards are updated for that platform.

Note: The manager, Corporate Information Security Office (CISO) Information Systems Security (ISS), is responsible for the update and distribution of server hardening standards

10-2.3.2 Web Servers

All Postal Service Web servers, regardless of location, must use approved hardware and software with standard configurations to reduce likelihood of loss or compromise due to exploitation of configuration vulnerabilities. For Web or Internet projects under the direct control of the Postal Service, the development and testing must be conducted on specifically designated development Web servers. Web servers must not be implemented on individual workstations without prior written approval by the manager, CISO ISS.

10-2.3.3 Database Servers

Database servers must use security controls appropriate for the level of sensitivity and criticality of the information they contain. Database servers must be separate from other servers, including Web and application servers (see 10-2.3.4, Combined Web and Database Servers, for an exception).

Database servers located inside Postal Service firewalls must not be directly accessible from Web servers or other systems located outside firewalls. All database servers must be approved by the Network Change Review Board (NCRB) prior to being deployed to the demilitarized zones.

Database servers must not be deployed to a production environment before hardening.

10-2.3.4 Combined Web and Database Servers

A Web server and database server may be placed on the same host if all the following requirements are met:

a. Application is not sensitive-enhanced, sensitive, or critical.

b. Application is not Internet accessible.

c. Application is not on the DMZ.

d. Application is not enclaved with sensitive-enhanced, sensitive, or critical applications.

e. Application is operationally standalone, that is, does not interact with other database servers.

f. Host meets Postal Service server hardening standards.

10-2.4 Workstations and Mobile Computing Devices

All workstations and mobile computing devices including desktops, laptop computers, notebook computers, and tablet computers must have appropriate security controls. Workstation and mobile computing device installation and deployment must comply with standard configuration and deployment standards unique to that platform. All personnel are responsible for protecting the information resources at their individual work location and abiding by all information security policies and procedures that apply to their individual environment.

All Postal Service workstations and laptops must have an approved personal firewall installed and personnel must connect to the Postal Service intranet at least once per week to receive the latest software patches, antivirus pattern recognition files, and personal firewall patterns. Appropriate configuration of the workstations and laptops to receive these patches and pattern updates is required.

All workstations processing PCI information and all laptop computers, notebook computers and tablets must implement full disk encryption. In addition, sensitive-enhanced, sensitive, and critical information on other mobile computing devices must be protected (e.g., encrypted) when leaving a secure environment. All media subject to loss or removal from Postal Services premises must be encrypted. Only procure Postal Service approved devices from approved sources. Only use USB flash drives and removable media that are encrypted. Back up critical information frequently and send backups offsite in accordance with Postal Service procedures. Critical information must not be backed up on the same device as the primary information.

10-2.4.1 Physical Security

All Postal Service workstations and mobile computing devices must be protected, at a minimum, by secure physical access to the facility or room. Other physical security controls may include, but are not limited to: unique platform identification (inventory control), identification card reader, screen

protector or positioning screen to restrict viewing from passersby, lockable keyboard, physical lock, and desk-fastening security equipment.

10-2.4.2 Password-Protected or Token-Protected Screen Saver

Where feasible, all workstations and mobile computing devices must be configured prior to deployment to use password-protected or token protected screen savers. After a period with no activity, password-protected screen savers will blank the screen; a password or token is then required to resume work. Users must protect the screen saver password or token just as they protect all other system passwords.

10-2.5 Mobile Computing Devices

Mobile computing information resources must be protected against damage, unauthorized access, and theft. All personnel who use or have custody of mobile computing devices, such as, handheld computers, smart phones devices, wireless telephones, and removable storage media devices, are responsible for their safekeeping and the protection of any sensitive-enhanced, sensitive, and critical information stored on them.

All laptop and notebook computers must implement hard disk encryption. In addition, sensitive-enhanced and sensitive information on other portable devices must be protected (e.g., encrypted) when leaving a secure environment. All media subject to loss or removal from Postal Services premises must be encrypted. Only procure Postal Service approved devices from approved sources. Only use USB flash drives that are capable of encryption.

All mobile computing devices must be managed by a Mobile Device Management (MDM) solution. The MDM solution must be vetted and approved by CISO.

Data on all mobile devices must be systematically eradicated before transferring to another individual or disposal.

10-2.6 Bring Your Own Device

Personnel must not load Postal Service information on their own computing device or connect their own computing device to the Postal Service network.

10-2.7 Hardware Asset Inventory

A comprehensive, accurate, and up-to-date Hardware Asset Inventory must be maintained and must include all technology assets known to the organization, with the potential to store or process information. This inventory must include all hardware assets, whether currently connected to the organization's network or not. The inventory must be capable of being dynamically updated using active or passive network discovery tools and other network configuration management tools such as Dynamic Host Configuration Protocol (DHCP).

The Hardware Asset Inventory must contain detailed identifying and technical information about each hardware asset in the inventory. This information must include, at the least, network address, hardware address, machine name, data asset owner, owner's department, and asset type. In addition, the

inventory must denote whether the asset has been approved for connection to the network.

10-3.1

10-2.7.1 Active Hardware Discovery

An active discovery tool must be used on a regular basis to identify all devices currently connected to the organization's network. The discovery tool must have the ability to actively scan the entire network upon demand. The active tool should update the hardware asset inventory with the results of this discovery, such that the inventory can report on those devices currently attached to the network.

10-2.7.2 Passive Hardware Discovery

A passive discovery tool must be used to identify and log all devices at the moment the device connects, or attempts to connect, to the network. The hardware asset inventory should be updated with the results of the passive logging, such that the inventory can report on the status of hardware assets upon their initial connection to the network.

10-2.7.3 DHCP Logging

Dynamic Host Configuration Protocol (DHCP) must be used to assign dynamic IP addresses and the assignment of these addresses must be logged and used to update the hardware asset inventory.

10-2.7.4 Hardware Asset Removal

Unauthorized hardware assets, as denoted in the hardware asset inventory, must be actively removed from the network or quarantined by assignment to a specific network segment. In addition, the asset inventory must be updated to reflect the exclusion or quarantining of the asset.

10-2.7.5 Network Access Control

Network Access Control (NAC) is the technique for network management and security that enforces policy, compliance and management of access control to a network. The Network Access Control (NAC) Process supports the Handbook (HBK) AS-805, Information Security Policy for Information Security Services.

Phase 1 – Authorize Hardware and Software into TIPA
The introduction of new devices and software into the USPS® environment must go through the appropriate activities for authorization. The authorization of hardware and software assets occurs in the Technology Initiative Prioritization Assessment (TIPA) Process. The TIPA Process evaluates all hardware and software assets seeking access to the USPS® networking environment and either approves or denies such requests.

Phase 2 – Authenticate Hardware and Software
After TIPA approval, Hardware and Software assets will be authenticated by undergoing the following:

a. Software will be verified through ITK, authorized application and code signing. Hardware will undergo port-level access control by utilizing the 802.1x authentication process to ensure a digital certificate signed by a USPS®

Certificate Authority (CA) is present on both the device and the authentication server.

b. Realizing that all devices don't support 802.1x authentication, security tools will interrogate all devices, pulling hardware and software attributes from the device to establish a unique fingerprint.
c. Upon TIPA approval, required asset data information will be supplied to CMDB.
d. Fingerprints will also be used to confirm that authorized devices adhere to USPS® compliance guidelines and apply the appropriate Network Access Control (NAC).

Phase 3 – Health Check
A health check is performed to provide ongoing monitoring to confirm assets are compliant as follows:

a. Monitor assets to confirm required capabilities are current and operational (i.e. end point protection, patching levels, hotfixes, etc.)
b. Perform Health Check on Hardware and Software Assets to identify end of life status for devices requesting access to the network.

Phase 4 – Security Monitoring of Assets
Once a device is authorized through an authentication process, the device shall be granted access to the network and will continue to be measured for compliance to USPS® Policy. Results will be monitored by the USPS® Cyber Security Operations Center (CSOC) Team as per the Cybersecurity Incident Response Plan (CSIRP).

CSOC enacts a multi-pronged approach to continuously monitor for possible cyber threats to the Postal network. The CSOC monitors the USPS® networking environment for all assets attempting connectivity and have the authority to block or quarantine any asset that does not comply with USPS® Policy.

Cybersecurity Compliance - To support the NAC Process, the CIS Critical Security Controls continue to be addressed to ensure only authorized computing devices and software are given access to the USPS® networking environment. The cybersecurity controls ensure all unauthorized computing devices are found and prevented from gaining access. This also ensures all unauthorized software is found and prevented from installation or execution.

Contact Information - The Information Security Executive Council provides oversight for the implementation and management of the Network Access Control (NAC) MI document. The Information Security Executive Council consists of appropriate Postal Service representatives and serves as a steering committee advising the CISO and promulgating information security throughout the Postal Service.

For questions about the Information Technology Asset Access Control Management Instructions, please contact the Corporate Information Security Office (CISO).

The following diagram illustrates the phases and activities for authorizing, authenticating and monitoring computing devices and software requesting or requiring access to the USPS® networking environment.

Approval Phase	Authentication Phase	Health Check Phase	Security Monitor Phase

Hardware and Software	Hardware	Hardware	Hardware and Software
• Technology Initiative Prioritization Assessment (TIPA) Process • Approve or Deny • Register in ITK or CMDB	802.1 x Authentication (Port Level Access Control) Fingerprinting Configuration Management Database (CMDB) Assets	Fingerprint – OS, make, model	• CSOC authority to identify incidents • Apply appropriate controls, e.g., restrict, deny or quarantine Anything failing could be quarantined
	Software	Software	
	• IT (Information Toolkit) • Authorized Application • Code Signing • Fingerprinting • Configuration Management Database (CMDB) Assets	• Ensure protection tools are up-to-date and in compliance, e.g., SEP, Tanium, SCCM, Cisco AnyConnect Anything failing could be quarantined	

~~The Postal Service must use port-level Network Access Control (NAC), based on 802.1x standards, to control which hardware assets can authenticate and connect to the network. The authentication system must be tied into the hardware asset inventory to ensure that only authorized devices, as noted in the inventory, are allowed to connect to the network.~~

10-2.7.6 **Client Certificate Authentication**

The organization must use client x.509 digital certificates to authenticate hardware assets connecting to the organization's trusted network.

10-3 Software and Applications Security

Security attributes and capabilities must be considered in the purchase/ acquisition or development of all Postal Service software. The collection of

features of the operating system, application, database management system, and utility software must be complementary and enhance the security of the system.

10-3.1 Software Safeguards

Software configuration and installation must include only the features, services, and functions necessary to perform the required business activities.

Controls must include, but are not limited to, the following:

a. Activating or enabling all safeguards embedded in computer software to restrict access to authorized users, maintain system performance, and to monitor for suspicious activity.

b. Documenting information security settings in the security plan and updating the settings during the software lifecycle to continuously provide required level of protection.

c. Disabling or removing all features and files that have no demonstrable purpose.

d. Disabling or removing default privileged log-on IDs, changing all default passwords, and removing guest accounts.

e. Removing test data.

f. Prohibiting use of administrative and root accounts for running production applications.

g. Limiting access to the specific files required.

h. Restricting access to systems software utilities to a limited number of authorized users on the basis of need-to-know.

i. Syncing privileges with various application roles.

j. Using HTTPS to secure the credentials on Web login pages.

k. Using Postal Service certificates on internal HTTPS Web pages.

l. Including the Postal Service logo on the initial application Web page.

m. Using only Postal Service standard encryption. If an encryption solution is not compliant with the current Postal Service standard, then either an EAC review or an exception must be requested.

n. Disabling directory enumeration on the servers.

o. Reviewing software for unauthorized products quarterly.

For PCI in scope applications, the following controls must also be included:

a. Prohibiting the caching to workstations the following file types: doc, txt, pdf, html, htm, tif, gif, jpeg, jpg, xls, etc.

b. Prohibiting the ability to enter an application Web URL and pull data from the application without authentication.

c. Implementing only one primary function per server.

10-3.2 Complying With Copyright and Licensing

All software used on Postal Service information resources must be purchased in accordance with Postal Service policies and procedures and be

licensed and registered in the name of the Postal Service. All personnel must abide by software copyright laws and must not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

10-3.3 Secure-Transaction Compliance

10-3.3.1 Financial Requirements

Financial requirements must be implemented when processing e-Commerce financial transactions (Note: these requirements are set by the payment card industry).

10-3.3.2 Medical Information Requirements

Appropriate security requirements must be implemented when processing health or medical information.

10-3.4 Version Control

All software that can be modified must be managed through the authorized Postal Service change control and management process (see 10-5, Configuration and Change Management). Software containing modifications, such as exits and supervisor calls, must be documented detailing the extent of the modifications. The modifications must be fully reviewed, tested, documented, and installed in a controlled environment to avert possible adverse effects on the security of the production environment.

10-3.4.1 Updating Software

Only authorized personnel may perform updates to the production application programs or operating system libraries/directories.

Individual access privileges must be approved by appropriate management officials.

After the system is changed, the security controls must be checked to ensure the security features are still functioning properly. Periodically (at least annually) the security controls must be tested to ensure the information security controls are functioning as designed and documented.

Significant change will cause the reinitiation of the C&A process. The criteria for recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process,* 6-2.

10-3.4.2 Distributing Software

Controls must be in place to regulate and manage the distribution of Postal Service system-wide production applications to field sites. These controls must ensure that the correct version is installed on all nodes and that the code cannot be modified on the field computer systems.

10-3.4.3 Prohibited Software

Do not install software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software.

Software no longer on the infrastructure toolkit (ITK) must be removed from the Postal Computing Environment (PCE). Use of unsupported software

must be approved by IT management and maintained by IT or one of IT's contractors, or removed from the PCE. Direct all requests for software not on the ITK to the Enterprise Architecture Committee (EAC) (see 10-4.2, *Acquiring Hardware and Software).*

10-3.4.4 Unapproved Software

Unapproved software is removed by the IT staff. The Postal Service must ensure that unauthorized software discovered during software inventory scans is deinstalled or if the software is unknown or inaccurately noted as unauthorized, then the software inventory must be updated accordingly.

10-3.4.5 Source Code

Acquired mission critical software will include source code where feasible. A written consent of the authorizing official is required for exceptions to this source code requirement. The acquisition and use of binary or machine executable code without the source code must be accompanied with a vendor warranty.

10-3.5 Operating Systems

All Postal Service information resources must use approved vendor-supported operating systems, including all approved updates and patches. Operating systems must have controls in place to prevent a compromise of the integrity of the computer operating system environment and must be configured to comply with operating system security requirements specified by Postal Service policies. All information resources using vendor-unsupported operating systems must maintain risk acceptance documentation as specified by 10-4: General Policies for Hardware and Software.

10-3.6 Application Software

Postal Service information resources must use only approved application software. Application software must be compatible with installed security software. Security activities for application software must be incorporated in the applicable life-cycle process during development. Application software developed in house or outsourced is subject to the C&A process.

10-3.7 Database Management Systems

All Postal Service information resources must use Postal Service-approved database management systems (DBMSs) that have been configured to comply with Postal Service security policies including:

a. Implement role-based access.

b. Authenticate all access by information resources, administrators, and users.

c. Prohibit direct SQL queries to the database.

d. Prohibit database servers located inside Postal Service firewalls from being directly accessible from Web servers or other information resources outside those firewalls.

10-3.7.1 DBMS Activity Journals

Each production DBMS must have a journal file to protect against accidental destruction of data or interruption in service. Journal files must be backed up as specified in the DBMS or the applicable business continuity plan.

10-3.7.2 DBMS Security Features and Views

All database tables must utilize the security features of the DBMS or the platform access control software (e.g., mainframe) to preserve the integrity of the database. Views and discretionary access controls must be used to protect sensitive-enhanced, sensitive, or critical information and enforce need to know.

10-3.8 Web-Based PCI Applications

Web-based PCI applications must deploy an application firewall in front of the Web site or hire a qualified third party to evaluate the Web-facing applications in accordance with the current PCI DSS.

10-3.9 COTS Software

Commercial-off-the-shelf (COTS) software must be purchased from a Postal Service-approved source. The EAC approves COTS software for use within the Postal computing environment. Requests for unapproved COTS software must be submitted to the EAC for review and approval.

Computer software purchased for the Postal Service must be registered to the Postal Service. COTS software used within the MPE/MHE non-routable address space environment is approved by Engineering.

COTS software used to process payment card information must be in certified by a Payment Application Qualified Security Assessor. The certification status of the COTS software must be checked prior to acquisition and before major new software releases are installed.

10-3.9.1 COTS Software Security Evaluation and Vulnerability Assessment

A COTS software security evaluation and vulnerability assessment must be performed for all proposed additions to the Postal computing environment. It is recommended that the COTS vulnerability assessment be updated for COTS software associated with sensitive-enhanced, sensitive, and critical information resources when first installed and for every version update.

10-3.9.2 COTS Independent Code Review

COTS applications that contain custom programming or scripts may be subject to an independent code review. An independent code review examines the custom source code and documentation to verify compliance with software design documentation, programming standards and to ensure the absence of malicious code. COTS custom programming or scripts may require a code review. COTS modification without authorization by the EAC is prohibited. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for the criteria for conducting an independent security code review.)

10-3.10 Browser Software

10-3.10.1 Approved Browser Software

Workstations and applicable mobile computing devices should use Postal Service-approved standard browser software. Web applications developed for Postal Service use must be compatible with Postal Service-approved standard browser software. The software must support encryption and comply with the privacy and cookie policies found at www.usps.com.

10-3.10.2 Cookies

Cookies are defined as:

a. Session cookie is a small piece of textual information that a server places temporarily on your browser during the time your browser is open. The cookies are erased once you close all browsers.

b. Persistent cookie is a small piece of text stored on a computer's hard drive for a defined period of time, after which the cookie is erased. The Postal Service must not collect or link to personal information through persistent cookies without customer's express consent.

Use of cookies on externally facing websites is detailed in Postmaster General Letter on Cookie Usage dated 23 January 2008 and is restricted to the following:

a. Session cookies may be used to support transactions, logging on and off the site, and computing postage.

b. Persistent cookies are allowed for the following limited purposes:

(1) To gather non-personal usage statistics such as how many new, repeat, and total visitors use our Web site.

(2) To support advertisements or promotions.

(3) To recognize customers or their information on a return visit, but only if they have expressly told us they want to be so recognized.

c. Further detailed information on allowable use of cookies is contained in the USPS privacy policy at http://about.usps.com/who-we-are/ privacy-policy/welcome.htm

10-3.11 Third-Party Software

Third-party software is defined as follows:

a. Software developed for the Postal Service by a vendor, contractor, supplier, or other third party.

b. Other limited-distribution custom-built applications.

c. COTS software that has been modified with custom programming scripts or languages.

10-3.11.1 Ownership

Third-party software developed under contract or funded by the Postal Service must be considered the property of the Postal Service unless otherwise stated in the contract.

10-3.11.2 Licensing and Escrow of Custom-Built Applications

Third-party software not owned by the Postal Service but considered a required component of an information resource used in an essential business activity must be licensed to the Postal Service. The vendor of this software must escrow the source code for each new version submitted to the Postal Service. This escrow requirement must be included in the contract's Statement of Work.

10-3.11.3 Assurance of Integrity

A written integrity statement must be provided with significant third-party software that provides assurances that the software does not contain undocumented features or hidden mechanisms that could be used to compromise the software or operating system security.

10-4 General Policies for Hardware and Software

10-4.1 Securing the Postal Service Computing Infrastructure

The Postal Service computing infrastructure must be protected through the implementation of information security standards, processes, and procedures.

Note: The manager, CISO ISS, is responsible for developing and maintaining an Enterprise Information Security Architecture and coordinating a secure Postal Service computing infrastructure by setting standards, and developing and/or approving the security processes and procedures.

10-4.2 Acquiring Hardware and Software

All hardware and software must be approved and purchased from approved Postal Service sources. Hardware and software not listed on the Infrastructure Toolkit (ITK) must be approved by the Enterprise Architecture Committee (EAC).

Only encrypted USB flash drives are approved for purchase. Encrypted USB flash drives, available from approved Postal sources, are the only USB drives authorized for use in the Postal environment.

All workstations and laptops must be capable of full disk encryption.

All removable electronic devices including laptops, notebooks, tablets, smartphones, external hard drives, and removable media must be encrypted.

10-4.3 Using Approved Hardware and Software

10-4.3.1 General Acquisition Policy

All Postal Service information resources must use only hardware and software purchased from approved Postal Service sources. All Postal Service information resources must use only software listed on the ITK.

Software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software must not be installed. Personnel wishing to use information resources not on the ITK must obtain approval from the EAC.

Engineering must approve hardware and software used within the Engineering private MPE/MHE network.

10-4.3.2 Shareware and Freeware

In addition to approval by the EAC, shareware and freeware must have a formal code review performed and must be scanned for viruses and malicious code and evaluated for security defects prior to use on any Postal Service information resource. Postal Service approved instances of share and freeware must be code signed, appropriately licensed, inventoried, and stored in a Postal Service repository for all future usages.

10-4.3.3 Teleworking

Where Postal Service non-public information is processed via teleworking, organizations should issue teleworkers a Postal Service ACE laptop.

10-4.4 Testing of Hardware and Software

Thorough testing of all new or modified hardware and software is required to ensure that there is no adverse effect on the security of Postal Service information resources.

10-4.5 Tracking Hardware and Software Vulnerabilities

Designated personnel in Customer Care Operations, Host Computing Services, Information Systems Security, and Engineering must be on hardware and software vendor advisory mailing lists and other forums appropriate to the information resources under their control. All vulnerability advisories involving hardware and software in use within the Postal Service computing environment must be documented and tracked.

10-4.6 Scanning Hardware and Software for Vulnerabilities

Scanning tools must have the ability to update the list of vulnerabilities to be scanned and must be scanned on a regular basis. The scanning procedure must ensure adequate scan coverage and update the list of vulnerabilities. Hardware platforms and software packages must be scanned on a regular basis. The scanning procedure must ensure adequate scan coverage and update the list of vulnerabilities.

For in-scope PCI externally facing applications, vulnerability scans must be performed quarterly by a PCI Approved Scanning Vendor (ASV). For in-scope PCI internal applications, vulnerability scans must be performed quarterly by a qualified resource.

10-4.7 Maintaining Inventories

10-4.7.1 Corporate Software Inventory

An enterprise-wide software inventory must be maintained. The enterprise-wide software inventory management process must ensure accountability and appropriate documentation. An accurate and up-to-date software inventory

must be maintained that includes all authorized software that is required in the enterprise for any business purpose on any business system. The software inventory must track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.

10-4.7.2 Individual Information Resource Inventories

All personnel are responsible for ensuring accurate inventories are maintained of Postal Service information resources assigned to them including hardware, non-ACE software, firmware, and documentation. The inventory management process must ensure accountability and must include current copies of hardware and non-ACE software maintenance agreements, licenses, purchase orders, and serial numbers. The inventory must indicate the individual authorized to use the information resource. The category supports granting access to auditors or other authorized personnel. The business system owner (VP or ~~Mgr~~Mgrs.) grants access to auditors or other authorized personnel and the FSC (Functional System Coordinator) reviews and provides access. Information resources supporting PCI are labeled with information that can be correlated to the application purpose, owner contact information, and the personnel authorized to use the information resource.

Payment cardholder media must be inventoried and the inventory reconciled semiannually.

10-4.7.3 Vendor Software Support

The Postal Service must ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. ~~Unsupported software should be noted as such and marked as unauthorized in the inventory system.~~Software inventory should be continually monitored and updated in order to reflect any changes to a vendor's support for authorized software. Unsupported software should be marked as unauthorized, as the Postal Service should only authorize and install software which is currently supported by the vendor and which receives necessary security updates.

10-4.7.4 Dynamic Software Discovery

The ~~organization~~ Postal Service must use dynamic software inventory tools to automate the discovery and documentation of all software currently installed on all business systems.

The Postal Service should utilize a tool (such as ForeScout) that can enumerate installed software and compare this against the authoritative software inventory. ForeScout is a platform used to scan software being used and finds software out of scope of the current inventory. Deviations from the authorized baseline will generate an alert to the System and/or Network Administrator.

10-4.7.5 Asset Inventory Integration

The software inventory must be tied to the hardware asset inventory such that all devices and the software installed on those devices can be tracked from a single location. This will allow the ~~organization~~ Postal Service to track the location of all installed software.

10-4.7.6 Authorized Application Software ~~Whitelisting~~

The ~~organization~~ Postal Service must use authorized application ~~whitelisting~~ technology on all assets in order to ensure that only authorized software executes and all unauthorized software is prevented from execution.

10-4.7.7 Authorized Software Library ~~Whitelisting~~

The ~~organization's~~ Postal Service ~~whitelisting~~ authorized technology must ensure that only authorized software libraries are allowed to load into a system process. The Postal Service must use authorized software to prevent installation and execution of unauthorized software.

10-4.7.8 Authorized Software Script ~~Whitelisting~~

The ~~organization's~~ Postal Service ~~whitelisting~~ authorized software must ensure that only authorized, digitally signed scripts are allowed to execute.

10-4.7.9 Software Segregation

The ~~organization~~ Postal Service must ensure that physically or logically segregated systems are used to isolate and run software that is required for business operations that incur higher risk for the organization.

10-4.8 Isolation of Postal Service Information

Postal Service data must not be co-mingled with non-Postal Service data.

10-4.9 Using Diagnostic Hardware and Software

Diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers) must be used only by authorized personnel for approved purposes (see 14-3, Monitoring).

10-4.10 Controlling Preventive and Regular Maintenance

Preventive and regular maintenance (and repairs) must be scheduled, documented, and controlled whether performed onsite or remotely. Information system components containing sensitive-enhanced or sensitive information must be sanitized prior to removal from a Postal Service facility. Maintenance records must be reviewed in accordance with manufacturer specifications and/or organizational requirements. Where possible automated mechanisms are employed to schedule and conduct maintenance.

Preventive and regular maintenance must be performed only by authorized personnel. When maintenance personnel do not have the needed access authorizations, organizational personnel with appropriate access authorizations must supervise maintenance personnel during the performance of maintenance activities on the information system.

Accounts used by vendors to support and maintain system components are enabled only when needed by the vendor and monitored while in use. When maintenance is complete, the security controls must be tested to ensure all security features are functioning properly.

For critical information resources, service level agreements delineate the spare parts that must be maintained onsite for the repair of key information

system components and the allowable time period for repair following a failure.

10-4.11 Controlling Maintenance Tools

Information system maintenance tools must be approved, controlled, and maintained on a regular basis. Automated mechanisms are employed, where possible, to restrict use of maintenance tools to authorized personnel.

Maintenance tools brought in to Postal Service facilities must be inspected by maintenance personnel for obvious improper modifications. Media containing diagnostic and test programs must be checked for malicious code prior to use.

All maintenance equipment capable of retaining sensitive-enhanced or sensitive information must be sanitized before the equipment is removed from the Postal Service facility. If the equipment cannot be sanitized, it must remain in the Postal Service facility or be destroyed.

10-5 Configuration and Change Management

The Postal Service configuration and change management process applies to all Postal Service information resources regardless of where the information resource is hosted or managed. Security-related requirements for the following areas are presented in 8-2.4, Configuration and Change Management:

a. Configuration component inventory.
b. Standard hardened configurations.
c. Change/version control.
d. Patch management.
e. Security testing of the configuration.

10-5.1 Significant Changes

What constitutes a significant change is defined in Handbook AS-805-A, 6-2.

10-6 Protection Against Viruses and Malicious Code

All Postal Service information resources must be protected against the introduction of viruses and other types of malicious code that can jeopardize information security by contaminating, damaging, or destroying information resources. Malicious code includes harmful and other unwanted code such as viruses, worms, keystroke loggers, botnets, Trojans, trap doors, time

bombs, activity trackers, remote control agents, snoopware, spyware, and adware.

10-6.1 Virus Protection Software

10-6.1.1 Installation

Information resources within the Postal Service must comply with the applicable hardening standards. Where applicable, active virus protection software must be installed, enabled, and configured to generate log files.

10-6.1.2 Scanning

To ensure Postal Service perimeter security, Information Security Services conducts scans for malicious code on the firewalls, FTP servers, mail servers, intranet servers, Internet application protocols, and other information resources such as workstations as necessary. Scans must be conducted weekly for information resources processing PCI.

10-6.1.3 Updating

Centralization of automatic updates to virus software is critical to updating information resources with the latest version of virus detection software and updated files of virus types (signature files). The managers, computing operations/infrastructures, are responsible for ensuring that virus protection software and signature files are current and distributed to Postal Service information resources. Virus protection software and signature files must be updated when received from the vendor.

10-6.2 Other Protection Measures

10-6.2.1 Protecting Shared and Retrieved Files

All personnel must run virus protection software prior to using shared or retrieved files from workstations, laptops, removable media, and other information resources.

10-6.2.2 Evaluating Dynamic Code

A code review must be conducted on sensitive-enhanced, sensitive, or critical information resources that contain dynamic code such as ASP, JavaScript, PLSQL, or CGI scripts (see 8-5.6.2, Conduct Security Code Review). In addition to the code review, information resources that contain dynamic code may be subject to an independent code review (see 8-5.6.6, Conduct Independent Security Code Review).

10-6.2.3 Protecting Applications

All application software and supporting files must be protected such that an error will be generated if there is an unauthorized attempt to modify the software. All activities involving modification of software must be logged.

10-6.2.4 Creating Backups before Installation

To assist with the post-virus restoration of normal computer activities, all computer software must be copied prior to its initial usage, and such copies must be stored in a secure location. These copies must not be used for

ordinary business activities but must be reserved for recovery from computer virus infections, hard-disk crashes, and other computer problems.

10-6.2.5 Checking for Viruses Before Distribution

All software, information, or any other type of digital media must be tested to identify the presence of computer viruses and other malicious code prior to distributing to Postal Service organizations, personnel, businesses, or the public.

10-6.2.6 Intrusion Detection/Prevention

All information resources within the Postal Service must be protected against the introduction of malicious code. A layered-defense must be implemented combining network level Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Malware/URL protection, antispyware software, anti-virus software, a personal firewall, host anomaly detection/intrusion prevention software, spam and content filtering for inbound e-mail, pop-up blocker protection, and user education. Unauthorized personnel must not modify the configuration of host-based protection software.

10-6.2.7 Automated Mechanisms

Information resources must provide automated mechanisms to support the handling of information security incidents.

10-7 Operating System, Database Management System, and Application Audit Log Requirements

Operating system, database management system, and application audit logs must be sufficient in detail to facilitate reconstruction of security-related events if a compromise or malfunction is suspected or has occurred. For events where immediate attention is required, the audit utility may trigger alarms that are directed to the proper location for action.

Audit logs must be reviewed daily for potential security incidents and security breaches. The reviews may be made by automated methods. The audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified. (See 9-11, Audit Logging, for additional requirements.)

10-7.1 Operating System Audit Logs

Operating system audit logs must record security-related events. Operating systems must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of operating system integrity. Operating system software must have the capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction.

10-7.2 Database Management System Audit Logs

Database management systems must implement appropriate logging of security-related events.

10-7.3 Application Audit Logs

Sensitive-enhanced, sensitive, and critical applications that have logging capability must implement appropriate logging of security-related events.

10-7.4 PCI Audit Logs

PCI audit logs must be retained for a minimum of one year.

11 Network Security

11-1 Policy

The Postal Service network infrastructure must be protected at a level commensurate with its value to the Postal Service. Such protection must include the implementation of the physical, administrative, and technical security controls and processes that safeguard the confidentiality, availability, and integrity of the network and the data in transit in accordance with Postal Service policies and procedures. Network controls and processes are necessary to do the following:

Safeguard data traffic.

Detect and prevent unauthorized access.

Respond to computer security incidents.

Detect and correct transmission line errors.

Ensure message integrity throughout the system.

Provide network and data security.

Ensure that recovery procedures are in place and working.

Specify the appropriate auditing procedures.

The CISO enforcement policy is as follows:

a. Remediation timeline SLA.

b. Adverse action pending SLA not being met.

This policy applies to all information resources, technologies, services, and communications that are part of the Postal Service network, including the following:

a. All transmission technologies used on behalf of the Postal Service in Postal Service or non-Postal Service facilities [(e.g., local area networks (LANs); wide area networks (WANs); voice communications; videoconferencing systems; voice messaging systems; desktop video communications; satellite broadcasts; facsimile transmission; and all other transmissions over landline, wireless, or Internet-based networks].

b. All types of information and network services, data, voice, image, and multimedia communications, regardless of transmission technology.

c. Changes to mail process environment must be in accordance with Handbook AS-805 documentation. Any interaction and business conducted must be in accordance with documented processes found within Handbook AS-805G document.

The Postal Service prohibits the attachment of any non-approved network device, to include routers, switches, repeaters, wireless access-points, and

firewalls to any point of the network. Direct questions about whether a network device is approved to the NCRB via e-mail to *ncrb@usps.gov*. The Postal Service removes or disables non-approved network devices added to the network infrastructure.

11-1.1 Generic Information Security Architectural Standards Network Architecture

The Postal Service has defined generic information security architectural standards that must be adhered to when new IT products, services, or applications are purchased for use within the Postal Service IT network. There are two basic environments to be considered within the IT infrastructure:

a. Internally facing.

b. Externally facing.

11-1.1.1 Internally Facing Environment

The internally facing environment consists of hardware/software components that provide IT services to an internal only user community (e.g., Postal Service employees). In other words, the user must be on the "inside," "blue side" or ".gov" side of the Postal Service network to access the components. This environment would also permit business partner VPN and Postal Service VPN connectivity.

11-1.1.2 Externally Facing Environment

The externally facing environment consists of hardware/software components that provide IT services to an external user community. The external community is connected to the Postal Service network via a public internet connection. It is intended for Postal Service customers using Postal Service IT services such as *www.usps.com*. This community will have limited access to the "outside," "red side" or ".com" side of the Postal Service network. This environment from a network security perspective is considered hostile and extreme care must be taken to insure the Postal Service architectural standards are applied.

11-1.1.3 Enclaves, Tiers, and Zones

The basic concept of the architecture is that each environment is broken into enclaves. Enclaves are further broken down into three tiers. Specific enclaves and tier vectors can be referred to as Zones. Enclaves, tiers, and zones have degrees of separation dependent on the amount of risk each presents to the Postal Service network as a whole. The externally facing enclaves are considered high risk because they are connected directly to the internet. Enclaves with a high degree of risk use firewalls and "service separation" to provide a layered protection. Service separation, especially in the external, PCI, and sensitive-enhanced enclaves, is critical and must be understood by Postal Service application owners, hardware implementation teams, and vendors/suppliers providing services/applications to the Postal Service. Web services in the web tier must be separated from the application in the appropriate enclaves. The application must physically and logically reside on the application tier within these enclaves.

11-1.1.4 Externally Facing Websites

An HTTPS-only standard is used for all external-facing USPS web services Browsers and other HTTPS clients are configured to trust a set of certificate authorities that can issue cryptographically signed certificates on behalf of web service owners and communicate to the client that the web service host demonstrates ownership of the domain to the certificate authority at the time of certificate issuance. Internally issued certificates will not be permitted for web services whose users may not always be expected to trust the issuing federal certificate authority. These web services use a certificate issued from a publicly trusted certificate authority. The CISO is responsible for reviewing and approving, where applicable, requests for certificates from an external CA.

Externally accessible Postal Service web services must be protected through the following requirements, when available:

a. Hardening standards.

b. Application scans, code reviews, ~~V~~vulnerability scans, penetration testing, and vulnerability assessments.

c. Audit logs.

d. Content delivery network (CDN).

e. Web application firewall (WAF).

f. Automation/bot defense solution.

11-1.2 Network Infrastructure

The network infrastructure — facilities, equipment, services, protocols, and applications used to transmit, store, and process information — must be protected through the following requirements:

a. Physical security.

b. Network asset control.

c. Network configuration information.

d. Identification and authentication.

e. Authorization.

f. Hardening standards.

g. Secure enclaves.

h. Network isolation.

i. Vulnerability scans, penetration testing, and vulnerability assessments.

j. Firewalls.

k. Routers.

l. Demilitarized zones.

m. Network traffic monitoring.

n. Network connection.

o. Business partner and third party.

p. Remote access.

q. Network audit logs.

r. Wireless networks.

11-1.3 Wireless Network Security

Wireless technology, including wireless local area networks (WLANs), cellular technologies, radio frequency identifier (RFID) tag applications, Bluetooth technologies, and personal area networks, must be approved by the NCRB before purchase and integration.

11-2 Network Architecture

The network architecture — the appearance, functions, locations, and resources used in the network architecture — must be designed with the appropriate level of administrative and technical security controls, including the following:

a. Network addresses.

b. Network services and protocols.

c. Network perimeters.

d. Network integrity controls.

e. Time synchronization.

11-2.1 Network Addresses

All network names and addresses must be managed and approved by the central addressing authority within Telecommunications Services (TS). Internal network addresses must be protected, and access to internal network addresses is based upon a need to know and least privilege. When appropriate, TS conceals network addresses and provides translation of non-routable addresses.

11-2.2 Network Services and Protocols

All information resources must use only network services and protocols approved by the NCRB. All non-approved protocols and services must be disabled at the perimeter. Minimum requirements for extending the Postal Service intranet into the remote site are as follows:

a. Secure NCRB approval.

b. All connections to any network(s) other than the intranet must be controlled by firewalls managed by Postal Service TS or a TS designee.

c. Network changes to the agreed upon configuration must be approved by TS.

d. TS or a TS designee must have unrestricted physical access to the network.

e. All equipment connected to the network must meet current Postal Service security hardening standards.

f. Connections to the Postal Service intranet must be firewalled in a manner similar to current Postal Service secure enclave firewalling.

g. Business partner connections, including those that are an extension of the Postal Service intranet, must be Postal Service-managed via firewall or other network filtering device.

h. Passwords used to manage systems on the network must not be used to manage other systems or networks.

i. All remote site systems administrators must have a Postal Service security clearance.

11-2.3 Network Perimeters

Perimeters are clearly defined boundaries that must be established to securely control the traffic between Postal Service information resources and all other networks. All inbound or outbound network traffic must pass through appropriate access control devices, such as firewalls, before reaching Postal Service information resources. The manager, TS, must ensure perimeter monitoring and may block the Internet Protocol (IP) address of a computer performing hostile reconnaissance or attacks against Postal Service networks. Other appropriate defensive measures to protect the Postal Service information resources may be used, as approved by the manager, TS and/or the manager, CISO ISS.

Note: The Office of the Inspector General (OIG) manages, secures, monitors, scans, and supports its own network and information technology (IT) infrastructure. The OIG network connectivity to the Postal Service intranet must comply with the requirements and processes for NCRB-approved connectivity to the Postal Service intranet.

11-2.4 Network Integrity Controls

The manager, TS, establishes a system of controls to safeguard the data traffic, detect and correct transmission line errors, ensure message integrity throughout the system, and protect computers and other telecommunications endpoints. Adequate audit procedures must be employed to monitor and analyze network integrity.

11-2.5 Time Synchronization

All system (including servers) and network clocks must be synchronized to ensure all systems have the correct and consistent time

a. Based on International Atomic Time.

b. Time data is protected – access to time data is restricted and all changes to time settings are logged, monitored, and reviewed.

c. Time settings are received from an industry-accepted time source.

11-3 Protecting the Network Infrastructure

The network infrastructure consists of the facilities, equipment, services, protocols, and applications used to transmit, store, and process information. The Postal Service network infrastructure is protected through the following:

a. Ensuring physical security.
b. Maintaining network asset control.
c. Protecting network configuration information.
d. Implementing identification and authentication.
e. Implementing authorization.
f. Implementing hardening standards.
g. Determining when a secure enclave is required.
h. Establishing secure enclaves.
i. Isolating the Postal Service networks.
j. Conducting vulnerability scans, penetration testing, intrusion detection, and prevention capabilities.

11-3.1 Ensuring Physical Security

Servers and other components of the Postal Service networks must be located in areas secured to a level commensurate with the sensitivity and criticality of the information stored, processed, or transmitted. Access to network infrastructure components must be limited to authorized personnel.

11-3.2 Maintaining Network Asset Control

All infrastructure components must be inventoried at regular intervals and labeled for asset management and physical protection.

11-3.3 Protecting Network Configuration Information

Network information, including, but not limited to, configurations, addresses, subnet masks, secure enclave locations, and firewalls must be protected and treated as sensitive. Access to network configuration information must be based upon the security principles of need to know and least privilege.

11-3.4 Implementing Identification and Authentication

Personnel and information resources must be required to identify and authenticate themselves to the network before being allowed to perform any other actions on the network.

11-3.5 Implementing Authorization

Access to information resources must be granted based on the job function, appropriate clearance or background investigation, need to know, separation of duties, and least privilege.

11-3.6 Implementing Hardening Standards

Information resources supported by networking must be hardened to meet or exceed the requirements documented in Postal Service hardening standards specific to each platform. Hardening refers to the process of implementing additional software and hardware security controls. Hardening standards are based off of CIS sources, vendor recommended settings and industry best practices.

Note: The manager, CISO ISS, is responsible for the distribution of information resource hardening standards.

11-3.7 Determining When a Secure Enclave Is Required

Enclaves can be implemented to enforce separate security zones (e.g., to segregate information resources with similar issues and risks). An enclave is a virtual LAN configured to isolate a subnet/host system from other systems based on risks. All traffic in and out of the enclave is forced through a control interface.

Enclaves are required for the following information resources:

a. Information resources accessible from the Internet (i.e., externally facing information resources).

b. Information resources remotely managed by Postal Service business partners.

c. PCI information resources must be in a separate PCI compliant enclave.

d. Sensitive-enhanced information resources.

e. Sensitive and critical information resources where the risks warrant additional protection. Information resources designated as sensitive, or critical must be assessed by the manager, CISO ISS, to determine if the resource should reside in a secure enclave. A completed business impact assessment (BIA) and the architectural diagram must be submitted to the manager, CISO ISS, for review and determination of whether additional enclave protection is required.

11-3.8 Establishing Secure Enclaves

Secure enclaves are network areas where special protections and access controls, such as firewalls and routers, are utilized to secure information resources. Secure enclaves apply security rules consistently and protect multiple systems across application boundaries. Secure enclaves must be implemented as follows:

a. Place servers within the network based on the sensitivity of the data.

b. Prohibit development, SIT, and CAT servers from being on the same subnet as production servers.

c. Employ protection for the highest level of information sensitivity in that enclave.

d. Reside on network segments (subnets) separate from the remainder of Postal Service networks.

e. Use "network guardians," such as packet filtering or application proxy firewalls, to mediate and control traffic.

f. Set enclave server rules and operational characteristics that can be enforced and audited.

g. Allow only predefined, securable information traffic flows.

h. Restrict administration to a small, well-defined set of system administrators.

i. Employ intrusion detection systems and intrusion prevention systems.

j. Audit the network boundary controls through the performance of network scanning procedures on a regular basis.

k. Restrict sharing of physical devices for virtual machines among multiple enclaves.

11-3.9 Isolating Postal Service Networks

Postal Service networks must be isolated from non-Postal Service networks [e.g., business partner and vendor (supplier) networks]. Postal Service and non-Postal Service network devices must not be co-mingled. Non-publicly available Postal Service information must be isolated from non-Postal Service information (e.g., business partner and vendor information) in transit.

11-3.10 Conducting Vulnerability Scans, Intrusion Detection, Penetration Tests

Only personnel authorized by the CISO are permitted to conduct network scanning, intrusion detection, penetration testing, and vulnerability scans of Postal Service information resources. During audits and investigations, the OIG may conduct scanning, penetration testing, and vulnerability scans as deemed appropriate. The OIG has the authority to scan and conduct penetration testing and vulnerability scans on his or her own network and IT infrastructure. Reports resulting from these vulnerability actions are sent to the program managers with a copy to the Corporate Information Security Office/ISSO for each system. The ISSOs will include these vulnerabilities into Risk Mitigation Plans for each system or Risk Register.

11-3.10.1 Vulnerability Scans

Vulnerability scans are required to systematically examine an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Requests for vulnerability scans must be directed to the manager, CISO ISS, for approval. Vulnerability scans are conducted on Postal Service information resources by CISO ISS or their designee.

11-3.10.2 Intrusion Detection and Protection

Intrusion detection is required to monitor network and/or system activities for malicious activity. The main functions of intrusion detection/prevention are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. All policy configurations will be managed by CISO ISS.

Requests for intrusion detection must be directed to the manager, CISO ISS, for approval. Intrusion detection is conducted for Postal Service networks by CISO ISS or their designee. The OIG conducts intrusion detection at its discretion.

The intrusion detection process consists of the following:

a. Monitor the network for suspicious traffic.

b. Examine network traffic to identify threats.

c. Utilize one of three detection methods:

(1) Signature-based detection.

(2) Statistical anomaly-based detection.

(3) Stateful protocol analysis detection.

(4) Dynamic analysis.

d. Take appropriate actions to mitigate the detected threats. This includes, but is not limited to, the following:

(1) Produce alert.

(2) Reset current session with/without alerts.

(3) Drop current session with/without alerts.

~~11-3.10.3 Penetration Testing~~

~~Penetration testing is required to determine the effectiveness of security of an information resource configuration. Requests for penetration testing must be directed to the manager, CISO ISS, for approval. Penetration testing is conducted for Postal Service networks by the CISO ISS or its designee. The OIG conducts penetration testing on Postal Service networks at its discretion.~~

11-4 Internet Technologies

The Postal Service uses Internet technologies in the following environments:

a. Internet.

b. Intranet.

c. Extranet.

11-4.1 Internet

Access to the Internet from Postal Service information resources must be routed through Postal Service-approved access control technology (e.g., firewalls, proxies and IPS).

11-4.2 Intranet

An intranet is a network based on Internet technologies located within an organization's network perimeter. The Postal Service operates and maintains an intranet for the conduct of Postal Service business. Access control technology, such as firewalls and filtering routers, IDS, and IPS, must be used to protect the Postal Service intranet at the network perimeter to provide access control and support for auditing and logging.

11-4.3 Extranet

An extranet is a network based on Internet technologies that allows an organization to conduct business and share information among business partners, vendors (supplier), and customers. Business partners must comply with the requirements and process of the NCRB contained in the Handbook AS-805-D, *Information Security Network Connectivity Process.* Business partners must be limited in their access to the specific information resources identified in the network connectivity request that is approved by the NCRB.

11-5 Protecting the Network/Internet Perimeter

The perimeter between the Postal Service network and the Internet environments must be protected through the following:

a. Implementing Internet security requirements.

b. Implementing firewalls.

c. Implementing routers.

d. Establishing demilitarized zones (DMZs).

e. Implementing IDS/IPS services.

f. Monitoring network layer traffic.

g. Monitoring and inspecting application layer traffic.

11-5.1 Implementing Internet Security Requirements

Internet-accessible information resources, such as those residing on DMZs, must implement security requirements that include, but are not limited to, the following:

a. Securely partitioning each Internet-accessible environment (e.g., the intranet and extranet) from each other.

b. Using firewalls or filtering devices to screen and monitor incoming and outgoing traffic.

c. Supporting encryption to protect the storage and transmission of sensitive-enhanced and sensitive information.

d. Performing continual evaluation, testing, monitoring, and maintenance of the firewalls.

e. Applying real-time monitoring, auditing, and alerting to detect intrusion, fraud, abuse, or misuse.

Access control technology, such as firewalls and filtering routers, must be used to protect the Postal Service intranet at the network perimeter to provide access control and support for auditing and logging.

11-5.2 Implementing Firewalls

A firewall is a safeguard or type of gateway that is used to control access to information resources. A firewall can control access between separate networks, between network segments, or between a single computer and a network. A current-generation firewall is generally not a single component but a strategy composed of both hardware and software for protecting an organization's resources.

Direct public access between the Internet and the Postal Service intranet must be controlled by a firewall. A firewall must be installed at each Internet connection and between any DMZ (and all PCI enclaves) and the Postal Service intranet.

Secure NCRB approval in advance of establishing network connectivity to an information resource involving firewall changes.

Firewalls must implement Postal Service hardening standards. These hardening standards must be updated as new vulnerabilities are uncovered and updates are available. Firewall hardening standards must be reviewed and updated at least annually.

A firewall must also be installed at each connection between the Postal Service intranet and mail processing equipment and mail processing infrastructure (MPE/MPI) devices. MPE/MPI firewall rule changes do not require NCRB approval.

11-5.2.1 Firewall Configurations

Postal Service firewalls must be configured to do the following:

a. Deny all services not expressly permitted (i.e., deny all inbound and outbound traffic not specifically allowed).

b. Restrict inbound Internet traffic to Internet Protocol (IP) address with the DMZ (ingress filters).

c. Prevent internal addresses from the Internet into the DMZ. Use anti-spoofing commands and techniques to prevent internal addresses from being spoofed and passed from the Internet to the DMZ.

d. Implement dynamic packet filtering (i.e., only allow "established" connections into the network).

e. Secure and synchronize router configuration files (i.e., running configuration files and start-up configuration files used to reboot machines must have the same secure configuration).

f. Audit and monitor all services to detect intrusions or misuse.

g. Notify the firewall administrator and system administrator in near real time of any item that may need immediate attention.

h. Run on a dedicated computer.

i. Stop passing packets if the logging function becomes disabled.

j. Disable or delete all nonessential firewall-related software, such as compilers, editors, and communications software.

11-5.2.2 Firewall Administrators

Each firewall or logical group of firewalls must have adequate resources assigned for firewall administration. Firewall administrators are responsible for ensuring compliance with standards for configuration and approved services and protocols.

11-5.2.3 Firewall Administration

All Postal Service firewalls must be located in a controlled environment. Firewall configuration standards must include a description of roles and responsibilities for management of all components.

Firewall administration must be performed from the local console or via remote access if approved by the manager, CISO ISS, and appropriately secured through strong authentication and encryption. Firewall configurations must be protected and treated as sensitive. Access to firewall configuration information must be based upon the security principles of need to know and least privilege.

11-5.2.4 Firewall System Integrity

Firewall rule sets must be reviewed every 6 months. Firewall system configuration and integrity must be validated and tested monthly by the firewall administrator.

11-5.2.5 Firewall Backup

The firewall (e.g., system software, configuration data, and database files) must be backed up as determined in the appropriate business continuity plan.

11-5.3 Implementing Routers

A router is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. Routers connect two or more logical subnets, allowing interconnectivity with hosts on intranets and extranets.

11-5.3.1 Router Configurations

Postal Service routers must be configured to do the following:

a. Implement Postal Service network security controls.

b. Suppress router advertisements.

c. Disable the finger service on all routers.

d. Disable File Transfer Protocol [FTP] server on all routers.

e. Disable Hypertext Transfer Protocol [HTTP] server on all routers.

f. Disable the boot-up service on all routers.

g. Disable configuration auto-loading on all routers.

h. Disable Internet Protocol [IP] source routing on all routers.

i. Disable IP directed broadcasts when not required.

j. Disable service Packet Assembler Disassembler [PAD] on all routers.

k. Disable proxy Address Resolution Protocol [ARP] when not required.

l. Disable gratuitous ARP on all routers.

m. Disable Simple Network Management Protocol [SNMP] write access to the router.

n. Disable Transmission Control Protocol [TCP] and User Datagram Protocol [UDP] small server services.

o. Disable Berkley Software Distribution [BSD] commands on remote systems.

p. Enable TCP keep-alive messages.

q. Enable Cisco Express Forwarding (CEF) on all Cisco routers.

r. Filter Internet Control Message Protocol [ICMP] on external interface.

s. Configure Data Name System [DNS] servers as a client resolver.

t. Configure virtual private network [VPN] as a tunnel type VPN.

u. Log severity levels 0 through 6.

v. Block IPv6 routing header.

w. Block IPv6 Undetermined Transport.

x. Block inbound traceroute responses.

y. Block RFC1918 addresses.

z. Set routers to intercept TCP SYN attacks.

aa. Limit TCP connection request wait times.

ab. Restrict access to stored configuration files.

ac. Restrict IPSec traffic.

ad. Require a log or syslog statement that follows every deny, discard, or reject statement.

ae. Require all network infrastructure component resources have latest operating system release level.

af. Require SNMP version 3 or higher be installed.

ag. Restrict SNMP access by IP address.

ah. Block SNMP at all external interfaces.

ai. Classify and mark management traffic to ensure it receives preferred treatment at each forwarding device along the path.

aj. Restrict messages to the Syslog Server.

ak. Synchronize Run and Startup configurations.

al. Configure Console Port to time out in 15 minutes or less.

am. Encrypt In-band traffic.

an. Log In-band management access attempts.

ao. Configure SSH timeout to 60 seconds or less.

ap. Implement SSH Version 2.

11-5.3.2 Router Administration

Router rule sets must be reviewed at least every six months.

11-5.4 Establishing Demilitarized Zones

DMZs are network segments between intranets, extranets, and the Internet that provide increased security for data transfer between information resources, vendors (supplier), and the public. DMZ requirements include the following:

a. Web servers and electronic commerce systems accessible to the public must reside within a DMZ with approved access control implemented via a firewall or gateway.

b. Sensitive-enhanced, sensitive, and critical information must not reside within the DMZ. Sensitive-enhanced, sensitive, and critical information must be installed on an internal network zone (i.e., enclave segregated from the DMZ).

c. All inbound traffic to the intranet from the DMZ must be passed through a proxy-capable device.

d. Virtualization is not allowed in the DMZ.

11-5.5 Monitoring Network Traffic

The Postal Service network perimeter must be monitored for network connectivity, services, and traffic. Monitoring must be conducted on both active and inactive connections.

Firewalls and IDS/IPS should be part of the path requirements as part of Compliance and Monitoring requirements as follows:

a. 11-7, BP connectivity requirements.
b. 11-8, Third-Party network connectivity.
c. 11-9, Remote access requirements.
d. 11-11, Wireless Network requirements.

11-6 Network Connections

11-6.1 Establishing Network Connections

The NCRB must approve all system network access before connectivity is established to the USPS network. Systems with high or moderate impact values with respective confidentiality, integrity, or availability security objectives have unique identity and authenticate network devices before establishing a connection to the USPS network. All connectivity to the USPS network must be monitored and audited in advance of the establishment of network connectivity. Any connectivity to the Postal Service network must allow monitoring.

11-6.2 Requesting Connections

The NCRB provides the mechanism for requesting, reviewing, evaluating, and approving connectivity between non-Postal Service individuals and organizations wishing to establish connectivity to the Postal Service intranet.

11-6.3 Approving Connections

Requests for connectivity to the Postal Service intranet must be reviewed, evaluated, and approved by the NCRB. All requests for connectivity must follow and comply with the requirements identified in the NCRB request process described in Handbook AS-805-D.

11-6.4 Physical Protection of Network Connections

Physical access to publicly available network jacks must be restricted to authorized personnel and enabled only when needed. Disable unused network connections in areas such as conference rooms where visitors and unauthorized network users are not escorted.

11-7 Business Partner Connectivity Requirements

Business partner/contractor/supplier (business partner) connectivity must be requested and funded by a Postal Service sponsor.

Connections using either existing BP ISP connectivity or frame relay service directly connected to the Postal Enterprise are protected by firewalls and security processes that restrict business partners to the IP address or addresses, server or servers, and ports or protocols they are explicitly authorized to access.

Business partners must be limited in their access to the specific information resources identified in the network connectivity request that is approved by the NCRB. No business partner is ever granted "open access" to Postal Service computing resources. These connections must be based on least privilege for both source and destination address. The use of blanket rules, such as wildcard masks and subnets larger than /24, will not be permitted without additional approval.

To protect the integrity of the Postal computing environment, business partners must have written information security policies describing how they will protect their proposed connection to the Postal Service and must include a copy of these security policies with their NCRB request.

Business partners must comply with the requirements and process of the NCRB contained in the Network Connectivity Process ~~[link]~~ including, but not limited to, the following:

a. Initiating requests with the executive sponsor for access to the Postal Service intranet.

b. Complying with all Postal Service information security policies.

c. Allowing site reviews by the Inspection Service or CISO.

d. Allowing audits by the OIG.

e. Reporting any security incident immediately to CyberSafe and executive sponsor.

f. Notifying the executive sponsor when connectivity is no longer required.

g. The executive sponsor will notify CISO/NCRB and open a request to remove access within 7 days of connectivity no longer being required (SLA).

11-8 Limiting Third-Party Network Services

Network services approved for third-party connectivity must be governed by the principle of least privilege and limited to those services and devices needed to perform the business function requested. The default must be to deny all access except those services specifically approved by the NCRB. The default must be to deny all access except those services specifically approved by the NCRB. The principle of least privilege applies to both source and destination addresses. The use of blanket rules such as wildcard masks and subnets larger than /24 will not be permitted without additional levels of approval.

When establishing third-party connections, access controls and administrative procedures must be implemented to protect the confidentiality of Postal Service information resources. The third party must be responsible for

protecting its private network infrastructure and information and must not rely on the Postal Service to perform this function. Part of securing the connection should include the Postal Service ability to monitor and inspect traffic.

11-9 Remote Access Requirements

Remote access privileges are restricted to authorized personnel and must be approved by appropriate management through ~~eAccessARISe~~Access/ARIS before being granted. Remote workstations and laptops must be physically secured to prevent unauthorized access to the device and the Postal Service intranet.

The use of personal information resources to remotely connect to the Postal Service intranet must be approved and connectivity must be managed through an approved virtual private network (VPN) solution.

An automatic session disconnect must be implemented for remote access technology after the standard time-out requirement. (See 9-6.10.3, Time-Out Requirements (Re-authentication) for the standard.)

11-9.1 Authentication

Information resources should be capable of strong authentication on application or network connections requiring remote access. Remote access requires users or devices to authenticate at the perimeter or connect through a firewall. Remote user communications must occur through encrypted VPN channels. Where possible, the authentication should use ~~eAccessARISe~~Access/ARIS. Remote PCI-related access must implement two-factor authentication.

11-9.2 Virtual Private Network

A VPN provides end users with a way to securely access information on the Postal Service intranet over an untrusted network infrastructure or an untrusted public network such as the Internet. Postal Service VPN requirements include, but are not limited to, the following:

a. Any Postal Service VPN solution must provide end-to-end encryption and strong authentication capability.

b. Employees must submit an electronic request for computer access, or its equivalent, to obtain access to Postal Service information resources through a VPN.

c. Business partners requiring access to Postal Service information resources through a VPN must submit a formal request to the NCRB in accordance with Handbook AS-805-D, *Information Security Network Change Process*.

d. Any VPN solution used for business partner connectivity must be capable of filtering access to specific information resources, and the connection must allow monitoring.

e. Any computing device connecting to the Postal Service intranet through a VPN must implement an approved personal firewall configured to Postal Service standards, as defined by CISO.

f. The end user must use a Postal-approved device or remote connection method and has the responsibility to gain access and fund the Internet Service Provider (ISP) service when accessing Postal Service resources. The Postal Service does not provide recommendations for any local ISP access. Once a communication path to the Internet through the ISP has been established, the VPN session is initialized through the Internet to the Postal Service network.

g. Upon management approval, contractors with unique Active Directory (AD) credentials and two-factor authentication may use a shared ACE computer where work requirements do not support the assignment of an individual ACE computer.

11-9.3 Modem Access

Modem access for all information resources to and from Postal Service networks must be approved in writing in advance by the manager, CISO ISS, and must implement the information resource protection measures described below.

Note: Additional modem approval by the manager, CISO ISS, is not required for approved remote access services (e.g., VPN or point-to-point protocol (PPP).

Any workstation on the Postal Service intranet with approved modem access must:

a. Implement an approved personal firewall configured to Postal Service standards as defined by CISO ISS.

b. Disconnect from the Postal Service intranet prior to establishing alternate or additional connections to any network such as the Internet.

c. Initiate protection measures to ensure that the system has been cleaned of any malicious code prior to being permitted to connect to the Postal Service infrastructure.

d. Deactivate modem immediately after use.

11-9.4 Dial-in Access

All dial-in access to and from Postal Service networks must be approved in advance by the responsible Postal Service manager and implemented by the manager, TS. All approved dial-in access must be established through Postal Service centralized dial-in services.

11-9.5 Telecommuting

Personnel working at alternative work sites must only use Postal Service approved computer hardware, software, and virus protection software when working on Postal Service business, when sharing files with the Postal Service, or when communicating through phone lines or the Internet with the Postal Service. Any approved personal hardware must have the latest security patches installed, Postal Service-approved virus software installed

with the latest pattern recognition file, and, if connecting via the Internet, a Postal Service-approved personal firewall must be implemented.

11-9.6 Remote Management and Maintenance

To protect the integrity of the Postal computing environment, use of remote administration and maintenance software and associated security controls must be approved by the manager, CISO ISS, in cooperation with the requesting organization.

Remote management and maintenance must be controlled and activity logs maintained. The remote access links, frequency of access, and associated controls must be documented in the security plan for the information resource. Two-factor authentication must be implemented and all communications must be encrypted. Vendor maintenance accounts must be enabled only when needed. When remote management and maintenance is completed, the remote access connection must be disconnected and disconnection verified.

Organizations performing remote access must implement the same general level of security as the system being accessed. Instances of remote management and maintenance must be audited on a regular basis.

11-10 Network Audit Log Requirements

Networks including firewalls and controlled interfaces must have an audit capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction. Network audit logs must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of network integrity. Network audit logs must be sufficient in detail to facilitate reconstruction of security-related events if a compromise or malfunction is suspected or has occurred. For events where immediate attention is required, the audit utility must trigger alarms that are directed to the proper location for action.

Network audit logs must be reviewed daily for potential security incidents and security breaches. The reviews may be made by automated methods. Audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified. (See 9-11, Audit Logging, for additional requirements.)

11-11 Wireless Networking Requirements

Wireless devices and the supporting network infrastructure are subject to the following wireless security requirements and standards: a. Wireless baseline requirements.

b. Wireless solutions.

c. Standard wireless solution.

d. Process for requesting nonstandard wireless solutions.

e. Bluetooth and personal area network applications.

f. Wireless LAN device management.

g. Compliance and monitoring requirements.

h. Firewalls and IDS/IPS.

Note: This policy does not cover wireless devices (e.g., cellular phones, pagers, and radio systems) unless they transmit data (see MI AS-8602003-2, Data Stewardship: Data Sharing Roles and Responsibilities).

11-11.1 Wireless Baseline Requirements

The following baseline requirements are key to ensuring basic functionality, maximum bandwidth, and appropriate network security:

a. Wireless applications must be capable of "mutual" device and user authentication (i.e., the device, the user, and the network must recognize each to be who they say they are).

b. There must be a secure link between a device and an access point (AP).

c. In addition to approval by the EAC, all wireless technology must be approved by the Spectrum Management Office before any implementation activities are initiated.

d. The installation of access points, wireless cards, or any wireless technology must be approved in advance by the manager, Telecommunication Services, and the NCRB because of the risks such installations can introduce to the Postal Service intranet, networks, and all connected information resources.

e. Telecommunications Services is authorized to deploy the standard wireless solution without additional approvals.

f. Wireless and wired networks must be developed and maintained separately and distinctly. A firewall is required between the wired and wireless network segments if Postal Service certificates are not used to Connecting APs or using wireless technology without proper prior approval introduces an unacceptable risk to the Postal Service intranet and other assets. Non-approved wireless technology must be removed from the Postal Service computing environment.

11-11.2 Wireless Solutions

Wireless technologies enable one or more devices to communicate without physical connections — without requiring network or peripheral cabling. Wireless technologies use the radio frequency spectrum to transmit data and such technologies present security-related challenges. Wireless solutions are grouped as follows:

a. Standard wireless solution.

b. Nonstandard wireless solution.

Devices that meet the current WLAN standard solution do not require a firewall between wireless devices and wired networks. All other devices require a firewall between wireless devices and wired networks.

11-11.3 Standard Wireless Solution

11-11.3.1 General Requirements

This standard technology solution is predicated on the implementation of the following general requirements:

a. Assurance that the device is authorized to access the Postal Service network domains.

b. Assurance that it is a Postal Service-managed device using approved virus protection, security patches, and personal firewalls.

c. Authentication of the user through Active Directory (AD) credentials.

d. Mutual authentication of device/client and remote authentication dial-in user service (RADIUS) server through Postal Service internal Certification Authority (CA) machine certificates.

11-11.3.2 Architecture Requirements

Wireless solutions must be compliant with the Mobile Computing Enterprise Architecture. The complete Architecture document can be found in the following documents folder: *http://it.blueshare.usps.gov/sites/itmc/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitmc%2FShared%20Documents%2FMobile%20Architecture%20and%20Strategy%20Documents*

Technical requirements for standard wireless architecture solutions are:

a. The standard architecture for WLAN authentication/encryption must be a Postal Service device capable of using:

(1) A Postal Service internal CA machine certificate authenticating to AD.

(2) Temporal key integrity protocol (TKIP) encryption.

(3) Wi-Fi Protected Access 2 (WPA2) or higher based on best practices for key management.

(4) Application and network device owners using PKI-based encryption on any wireless device implement and maintain a key management plan as identified within this policy document and approved by CISO.

b. Users must authenticate to AD and be authorized for wireless access.

c. Users and devices must be registered members of AD.

d. Users must be able to authenticate using AD credentials.

e. Devices such as workstations must be able to mutually authenticate to a RADIUS server using Postal Service Internal CA certificates.

f. The technology solution must use an approved supplicant client and the device must be a Postal Service device.

g. Clients must be able to download, store, and use a Postal Service internal CA machine certificate.

h. Protocols (e.g., PEAP) capable of supporting Postal Service machine certificates must be used.

i. Workstation/wireless card clients must be registered for central device management.

j. Drivers and cards must be compatible with Postal Service standards and certified by TS for use within the Postal Service network.

k. Service set identifier (SSID) standardization must be implemented to support mobility.

l. Firewall segmentation must be implemented at the demarcation of wireless networks to mitigate the risk of attack through compromised wireless networks.

11-11.3.3 How to Request Standard Wireless Services

Standard wireless connectivity is requested as follows:

a. Wireless infrastructure must be requested through TS.

b. Wireless infrastructure must be deployed, documented, and managed by TS.

c. Wireless cards/client devices must be purchased via Postal Service processes and contracts. The acquisition of mobile computing devices must be approved through IT Mobile Computing.

d. User wireless services must be requested via ~~eAccessARIS~~eAccess/ARIS at ~~*http://eAccessARIS.*~~ *https://eaccess.usps.gov*

11-11.4 Process for Requesting Nonstandard Wireless Solutions

The following process must be followed for business solutions including the use of wireless technology that do not meet the standards previously defined:

a. Obtain NCRB approval to proceed. Before pursuing a nonstandard wireless technology solution, approval to proceed from the NCRB must be obtained. The NCRB requires a business case for the alternate solution. The NCRB dictates the non-negotiable standards that the alternate solution must be compliant with.

b. Develop an architecture design. Develop an engineering architectural design in conjunction with TS. TS should validate compliance and functionality of the design to ensure that it will not adversely affect the current Postal Service solutions. TS will submit the solution design to IT Mobile Computing for review to ensure compatibility with the overall managed mobile computing technical architecture and strategy.

c. Obtain NCRB approval of the architectural design.

(1) Obtain approval of the application, the engineering architecture, and all wireless devices from the NCRB.

(a) For implementations involving MPE/MHE, contact the responsible design engineering organization that will send an e-mail to *NCRB@email.usps.gov* or submit a request through the NCRB Web site. The design engineering organization may also present the MPE/MHE project to the NCRB.

(b) For other implementations, contact the Business Relationship Management portfolio manager who will send an e-mail to *NCRB@email.usps.gov* or submit a request through the NCRB Web page on the IT Web. The Business Relationship Management portfolio manager will also act as a presenter to the NCRB on the requestor's behalf.

(2) At a minimum, the NCRB will evaluate against the following criteria prior to approval for implementation of wireless technology:

(a) Proper naming with regards to SSID.

(b) SSID broadcast turned off.

(c) Encryption of data between a device and an access point, or an ancillary downstream device. The majority of wireless APs have some inherent encryption capabilities.

(d) Trust between wireless devices. When setting up APs, there should be appropriate authentication — particularly a mutual authentication mechanism between a wireless device and an access point (802.1x) and user-based authentication when applicable (i.e., two-factor).

(e) Appropriate logging/intrusion detection on the wireless segment, either on the access point or related device.

(f) The requirement for whether a firewall is needed between the wireless AP and WAN.

(g) Centralized, secure administration using unique user name and passwords that are compliant with Postal Service policy. Ideally, all wireless user accounts should be located in a common repository.

(h) Firewall and virus protection implementation on devices.

(i) Request through ~~eAccess~~ARISeAccessARIS if Postal Service Internal CA machine certificates are required.

(j) Devices are remotely manageable by TS.

d. Obtain a wireless site survey. A wireless site survey must be performed to obtain maximum benefit of the wireless devices and to maintain appropriate security. TS arranges for the site survey via the Postal Service intranet contract. Normal turn-around time is 62 days; expedited is 30 days. The survey results will place the APs, offer channel sections, and specify other physical and programming parameters.

e. Acquire, program, and install device. After NCRB approval and review of the site survey report, the wireless infrastructure devices may be purchased by the customer through TS, who will then configure the devices. When the devices are programmed, they are sent to the site ready to be installed by the Postal Service intranet vendor.

11-11.5 Bluetooth and Personal Area Network Applications

Postal Service initiatives using Bluetooth and personal area networks require approval from the NCRB prior to deployment.

All implementations of Bluetooth and personal area networks must meet the requirements for a nonstandard wireless solution and the following requirements:

a. Radio frequency range must be managed, using only the minimum signal required, to perform the task and checked semiannually for confinement.

b. Device pair bonding (mutual authentication) must be used. Ensure the Bluetooth bonding environment is secure from eavesdroppers. If the authenticator (e.g., PIN, password, and shared secret) meets Postal Service aging and storage requirements, the standard password criteria apply (see 9-6.1, Passwords), otherwise the authenticator must be complex and a minimum of 16 characters.

c. The link between devices must be encrypted during the authentication exchange process and also when sensitive-enhanced or sensitive information is transmitted. Use security mode 3.

d. Bluetooth or personal area networks configuration files must be checked semiannually to ensure the security policy is enabled on devices where the files are accessible by end users.

e. Personal use of Bluetooth on Postal Service premises must be approved by the user's vice president or his or her designee because of the potential for interference to Postal Service systems such as Surface Visibility and Yard Management.

11-11.6 Wireless LAN Device Management

TS or its designee remotely manage all devices that connect to the network using 802.11x technology, that incorporate TACACS, and have RADIUS authentication. Periodic software updates and product enhancements are downloaded to APs as required to improve performance and enhance security. Access point management also includes constant operating assessments of the device. Any malfunctions or loss of effectiveness generate an alert for resolution.

11-11.7 Purchasing Requirements

Purchasing requests for wireless hardware, software, and services must address the requirements stated in items a through s below in order to comply with the Postal Service wireless security policy. For any particular wireless application, all of the requirements may not apply. The security requirements should be included in purchasing specifications procurement documents to adequately protect the wireless application and reduce the residual risk to an acceptable level.

Procurements must be compatible with the Mobile Computing Enterprise Architecture. An extract of the Best Practices and Standards can be found in the following documents folder: *http://it.blueshare.usps.gov/sites/itmc/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitmc%2FShared%20Documents%2*

FMobile%20Architecture%20and%20Strategy%20Documents

Wireless devices should be capable of supporting the following requirements:

a. For devices intended for stationary deployment (e.g., in vehicles or on loading docks), capable of being solidly secured (e.g., to the vehicle or building). This requirement also applies to add-on modules.

b. Capable of requiring a "power-on" password prior to the device operating. This password is in addition to the specific user authentication password.

c. Capable of ensuring device authentication and strong (at least two-factor) user authentication. The wireless device must have the capability to be configured to query a secondary device for access when the primary server is offline.

d. Be Wi-Fi protected access (WPA) certified. Has built-in security features, including data link-level encryption, 802.1x-compliant authentication model, and regular rotation of encryption keys.

e. Contain secure authorization software/firmware.

f. Where extensible authentication protocol (EAP) is used, capable of proper password management (e.g., aging and complexity criteria). The wireless device must have the capability to support password changes in a pre-established timeframe.

g. Capable of ensuring that users can be securely authenticated when operating locally or remotely. The device automatically senses when it is operating in a connected manner and uses the proper authentication.

h. Capable of implementing mutual authentication between the device and an access point.

i. Capable of being Active Directory-compliant for authentication purposes. Exceptions must be documented.

j. Capable of logging events.

k. Capable of meeting the Postal Service minimum encryption standard.

l. Capable of providing a secure channel for access point administration.

m. Capable of supporting end-to-end cryptographic protection for transmitting sensitive-enhanced and sensitive information where the traffic traverses network segments other than the wireless segment.

n. Capable of dynamic encryption key rotation. The wireless device must have the capability to support rotation of encryption keys in a pre-established timeframe.

o. Capable of supporting a timeout mechanism that automatically prompts the user for a password after a period of inactivity. The period of inactivity must be configurable via the device set-up procedure and ignore the keep-alive process (pings or loop socket-to-socket packets) for automated programs.

p. Capable of deactivating all communication ports and network associations during periods of inactivity.

q. Capable of implementing a personal firewall on wireless clients.

r. Capable of supporting static IP addresses and dynamic host configuration protocol (DHCP) on remote wireless equipment.

s. Capable of shielding authentication credentials against interception through short interval "authentication tunnels" (i.e., TLS standard).

Technical support for the integration of the wireless devices into the Postal Service infrastructure with other technological initiatives must be scoped, planned, and available in a timely and accurate manner (e.g., remote access for MPI, structured wiring switches, and SEF access).

11-11.8 Deployment Requirements

It is imperative to carefully plan the deployment of wireless technology. It is much more difficult to address security once deployment and implementation have occurred; therefore, security should be considered from the initial planning stage through deployment and operation.

Fulfilling the requirements stated in this section will ensure compliance with the Postal Service wireless security policy. For any particular wireless application, all of the requirements may not apply. The information systems security officer (ISSO) must work with the executive sponsor to select the security requirements that must be implemented to adequately protect that application and reduce the residual risk to an acceptable level.

11-11.8.1 Administrative Security Requirements

Wireless infrastructure administrative security controls and management practices are crucial to operating and maintaining a secure wireless network. Wireless administrative security requirements are:

a. Do not install access points, wireless cards, or wireless devices to gain access to the Postal Service intranet without prior written approval from the NCRB.

b. Submit a detailed Security Plan to the NCRB along with the request for wireless connectivity.

c. Implement configuration/change control to ensure that equipment (e.g., access points) has the latest software release that includes security feature enhancements and patches for discovered vulnerabilities.

d. Review security-related mailing lists for the latest security vulnerabilities and alerts and respond accordingly.

e. Test software patches and upgrades.

f. Install security patches in a timely manner (within 30 days for information resources supporting PCI applications).

g. Use approved standardized configurations that reflect the information security policy and hardening standards to ensure consistency of operation.

h. Change system defaults that come with the wireless access points, including SSID, password, read/write community strings, and IP addresses set by the manufacturer.

i. Implement firewalls between access points and the wired network.

j. Conduct scans continuously to identify unauthorized access points and other devices that can disrupt the wireless network or compromise the security of the Postal Service intranet. For the PCI cardholder environment, the scans must be conducted quarterly.

k. Disable wireless devices not included in the authorized wireless inventory.

l. Conduct information security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies (including the fact that robust cryptography is essential to protect the "radio" channel, and that theft of equipment is a concern).

m. Ensure that users know where to report lost or stolen wireless devices.

n. Perform a risk assessment to understand the value of the assets that need protection and document the residual risk following the application of all security countermeasures in the wireless deployment.

o. Centralize wireless security administration and actively monitor user connections.

p. Turn off communication ports and network associations during periods of inactivity when possible.

q. Perform perimeter surveys to review and adjust radio transmit power settings to prevent spillover (i.e., the leakage of Postal Service wireless radio signals beyond the perimeter of Postal Service property).

r. Use non-intelligible SSID identifiers, cryptographic keys, and administrative passwords.

s. Access point information fields must not be populated with Postal Service-identifiable information.

t. Bridging must always be disabled on access points and on remote wireless equipment that also has wired connectivity.

u. Disable SSID broadcasts on all wireless equipment.

v. Minimize broadcasts from access points or broadcasts on a segment (e.g., access point connected to a wired hub), and limit access point associations.

w. Ensure no microwave ovens or cordless phones are within sufficient range to create interference on WLANs.

x. Install antivirus software and malicious and unauthorized content inspection monitors on portable wireless devices.

y. Ensure access control lists clearly identify application rights (authentication) for all wireless users.

z. Avoid placing sensitive-enhanced or sensitive information on a handheld device. Store sensitive-enhanced or sensitive information encrypted and delete it from the handheld device when no longer needed.

aa. Synchronize mobile wireless devices with the corresponding workstations regularly.

ab. Do not use Postal Service-owned equipment on home wireless networks without a personal firewall and virus protection.

11-11.8.2 Physical Security Requirements

Physical security controls should be implemented to mitigate some of the risks such as theft of equipment and insertion of rogue access points, including wireless network monitoring devices. Physical security controls (e.g., barriers, access control systems, and guards) are the first line of defense. Wireless physical security requirements are as follows:

a. Deploy physical access controls (e.g., photo ID, card badge readers) to the building and other secure areas to protect against tampering and theft.

b. Solidly fix devices not under continuous user control (e.g., left in vehicles or on loading docks) to the vehicle or building through the use of physical locks and cables to minimize the risk of loss or theft.

c. Stow handheld devices in locked rooms and cabinets especially when left unattended for long periods (e.g., overnight).

d. Secure add-on modules to minimize the risk of loss or theft, since they sometimes are as much of a target as the primary handheld device.

e. Ensure access points are physically secure from tampering.

f. Locate authentication servers in protected areas behind access points.

g. Where sensitive-enhanced or sensitive information is transmitted, ensure external boundary protection (e.g., a fence or locked doors) is in place around the perimeter of the building or buildings.

11-11.8.3 Technical Security Requirements

Technical security controls should be implemented to mitigate risks such as eavesdropping, traffic analysis, masquerading, replay, message modification, and denial of service. Wireless technical security requirements are as follows:

a. Implement a "power-on" password based on Postal Service standards for each mobile wireless handheld device.

b. Implement appropriate password management (e.g., aging) for all handheld devices.

c. Implement mutual authentication between a wireless device and an access point.

d. Implement authentication for users whether operating locally or remotely (i.e., authenticate to the device or to the network).

e. Provide only specific services (e.g., HTTP, HTTPS, and SMTP).

f. Control access between the WLAN and wired LAN with a firewall.

g. Implement timeout mechanisms that automatically prompt the user for a password after a period of device inactivity.

h. Implement nonrepudiation access check for financial transactions.

i. Use the wireless access point for access only.

j. Configure the wireless access point properly.

k. Set wireless access points at 1, 6, and 11 so they do not compete and interfere with each other. If a nonstandard channel is used, it will indicate a possible "man-in-the-middle" attack.

l. Routinely test the inherent security features (e.g., authentication and encryption) that exist in wireless algorithms to protect sensitive-enhanced and sensitive information.

m. Encrypt data between a device and an access point, or ancillary downstream device utilizing Postal Service minimum encryption standards.

n. Use a VPN to secure communication between WLAN and LAN resources.

o. Implement mandatory access control (MAC) address filtering.

p. Use a HTTP/SHTTP proxy to access the Internet.

q. Turn off ad hoc networking and ensure your wireless network interface card (NIC) remains in "infrastructure only" mode.

r. Use temporal key integrity protocol (TKIP) to provide data encryption including a pre-packet key mixing function, a message integrity check (MIC), an extended initialization vector with sequencing rules, and a rekeying mechanism.

s. Implement 802.1x and EAP to provide a framework for strong user authentication.

t. Employ Postal Service standard end-to-end cryptographic protection to transmit sensitive-enhanced and sensitive information over other network segments, including wired segments or the Internet.

u. Even when approved cryptography is used, employ additional countermeasures (e.g., strategically locating access points, firewall filtering, blocking, and installation of antivirus software) as required.

v. Employ automated key rotation.

w. Install personal firewall software on all mobile networked wireless devices.

x. Implement appropriate logging and intrusion detection where any wireless equipment is used.

11-11.8.4 Maintenance Security Requirements

Maintaining a secure wireless network and associated devices requires significant effort, resources, and vigilance. Wireless maintenance security requirements are as follows:

a. Maintain a full topology of the wireless network.

b. Label and keep inventories of the fielded wireless and handheld devices including MAC addresses and serial numbers.

c. Create frequent backups of data on mobile wireless equipment.

d. Perform quarterly security testing and vulnerability assessments of the wireless network.

e. Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.

f. Apply patches and security enhancements in a timely manner (within 30 days for information resources supporting PCI applications).

g. Vigilantly monitor wireless technology for new threats and vulnerabilities.

h. Install the latest antivirus software on mobile wireless equipment.

i. Implement a secure channel for access point administration.

j. Configure alerts to data volume, packet collisions, and retries.

k. Conduct site surveys and adjust radio transmit power settings to avoid transmissions beyond Postal Service-owned property.

l. When disposing of handheld devices that will no longer be used, sanitize memory to prevent the disclosure of sensitive-enhanced or sensitive information and clear configuration settings to prevent the disclosure of restricted network information. Where portable hard drives are used, sanitize the disk in accordance with this handbook.

11-11.8.5 Security Requirements for Using a Public Hot Spot

Personnel connecting to public WLANs in airports, hotels, restaurants and such must take the following precautions:

a. Turn off file and print sharing from your wireless device.

b. Clear your list of "preferred networks."

c. Turn off ad hoc networking and ensure your wireless card remains in "infrastructure only" mode.

d. When using a virtual private network to connect back to the Postal Service Intranet, disable split tunneling.

e. Use a personal firewall that detects malicious scanning of your wireless device.

11-11.9 Compliance and Monitoring Requirements

Security assessments and audits are essential tools for checking the security posture of a wireless technology and for determining corrective action to ensure the network remains secure. It is important to perform regular audits using wireless diagnostic hardware and software. Administrators should periodically check for rogue access points and against other unauthorized access.

Only authorized personnel may use diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers).

Dedicated wireless monitoring that performs a full traffic analysis must be implemented to identify wired and wireless security issues and respond appropriately.

12 Service Continuity Plan

12-1 Service Continuity Policy

Service Continuity (SC) consists of the alignment of Business Continuity Plans (including Emergency Action Plans) and Disaster Recover Plans. CIO SC enhances the operational resilience of CIO organizations, their systems, and processes.

The Service Continuity Plan develops the management and governance framework for Postal Service CIO organizations to prepare for, respond to, and recover from any event that disrupts, or threatens to disrupt, normal operations. This policy is applicable to all CIO Service Partners and Owners (see Chapter 2, Security Roles and Responsibilities).

This policy ensures creation of missing plans (including Postal Service Disaster Recovery (DR) Plans, Business Continuity (BC) Plans, Functional (FF) Plans, and Emergency Action Plans (EAP), as well as review of alignment or augmentation of existing plans, by the CIO organizations as defined and mandated elsewhere in this document (Handbook AS-805) and Management Instruction (MI) AS-280-2018-1, *Integrated Emergency Management Supporting Field Business Continuity,* (published January 2018).

This policy, its recommendations, and resulting products (plans) are in compliance with the following:

a. The National Institute of Standards and Technology (NIST) SP 800.34.

b. Homeland Security Exercise and Evaluation Program (HSEEP).

c. Postal Service *Employee Labor Manual* (ELM), 810, Occupational Safety and Health Program; 840, – Safety Awareness Program; and 850, Emergency Action Plans and Fire Prevention and Control.

d. MI AS-280-2018-1, *Integrated Emergency Management Supporting Field Business Continuity.*

Specifically, this policy provides for the: identification, prioritization, vetting, and approval of CIO VP High-Value Services (HVS); compliance with Federal and Postal Service standards and guidelines for recovery plan(s) documentation, maintenance (updating), testing, exercising, and evaluation (TT&E); and personnel training.

The CIO SC policy ensures development of all Postal Service CIO organization's (CIO, Business Services Organization (BSO), Corporate Information Security Office (CISO), Enterprise Analytics (EA), Engineering (ENG), Information Technology (IT), and Mail Entry and Payment Technology (MEPT)) capability to prepare for, respond to, and recover from any event

that disrupts, or threatens to disrupt, normal operations which depend on services provided through the CIO organization. The program improves organizational and technology resilience processes and capabilities to ensure critical CIO services continue during and after an incident and applies to all Postal Service functional organizational elements and personnel.

This is achieved through the establishment and implementation of standards and guidelines for CIO SC including emergency management, service continuity and disaster recovery activities, and standards and plans (operational risk). Its focus is based on the identification and prioritization of the CIO's and VP's high-value services and their recovery/hardening/ resilience through a governance program which ensures maintenance and training on service continuity.

Specifically, through the development, documentation, and implementation of testing, exercising and evaluation processes, and documentation which validate compliance (or noncompliance) to CIO service continuity standards, guidelines, and processes, and effectively address noncompliance and corrective action the developed strategies and plans to sustain functions during a disruption can be practiced.

Service Continuity Management (formerly Business Continuity Management) focuses on resilience. Resiliency is not a process, but rather an end-state for organizations in which the organizations have the ability to quickly adapt and recover from any known or unknown changes to the environment. The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions. Risk management, contingency, and continuity planning are individual security and emergency management activities that can also be implemented in a holistic manner across an organization as components of a resiliency program.

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope; however, because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the following basic descriptions:

a. Business Continuity Plan (BCP) is the documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. *https://csrc.nist.gov/glossary/term/business-continuity-plan*

b. Contingency plan normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

c. Emergency Response (ER) Plan serves as a documented, organized process to manage an unexpected or dangerous occurrence and limit negative impact.

Service Continuity Plan

d. Incident Response (IR): IR serves as a documented organized process to manage the aftermath of any incident. The goal is to limit negative consequences of the event.

e. IT Incident Response Plan (IT-IRP) serves as a process to address the aftermath of any technology event or incident and at a minimum includes: Incident Severity definitions, IT IR Procedure, Contact Information and Communications expectations.

f. Cyber Incident Response Plan (C-IRP normally focuses on detection, response, and recovery to a computer security incident or event.

g. Disaster Recovery (DR) Plan defines how work can be resumed after a disaster.

12-2 Service Continuity Plan Requirements

The purpose of business continuity plans are to ensure that business processes which rely upon personnel to perform specific functions will continue after an unplanned emergent event. This event may affect the prerequisite or dependent personnel, tools, or facilities and require that the function be relocated or that an alternate process be initiated.

Business Continuity Plans mitigate operational risk by doing the following:

a. Protecting personnel and identifying essential business processes during an incident or disaster.

b. Reducing the impact of an incident or disaster on facilities' personnel and business processes.

c. Satisfying business continuity needs as defined by USPS management and aligning with industry best practices and United States federal government requirements and guidance.

The minimum requirements for Business Continuity Plans are defined in the following documents:

a. ASM, 28, Emergency Preparedness.

b. Management Instruction (MI) AS-280-2018-1, *Integrated Emergency Management Supporting Field Business Continuity* (published October 24, 2016).

c. Federal Continuity Directive 1 (FCD 1), "Federal Executive Branch National Continuity Program and Requirements" dated January 2017.

All CIO managed facilities will use the structure, tools, products, and nomenclature of the integrated emergency management (IEMM / IEMP) discipline to include the following:

a. Emergency Management Team (EMT) concept of operations.

b. Integrated Emergency Management Module (IEMM) within the Facilities Database System for data entry.

c. Integrated Emergency Management Plan (IEMP) that consists of emergency action, fire prevention, and continuity of operations (COOP) plans, and emergency response checklists.

d. Business Continuity Preparedness (BCP) cyclical requirements for testing, training, exercise, and review.

e. IEMP update and certification requirements.

12-3 Disaster Recovery Plan Requirements

12-3.1 General

All Application and Infrastructure Service owners must develop Disaster Recovery (DR) plans to provide for the resumption of automated systems in the event that those systems are unable to operate as built. Application teams develop Application Disaster Recovery Plans (ADRP). These plans make a reference to dependent Infrastructure Services but recovery of those services is not in scope for the ADRP. Infrastructure Services develop Infrastructure Disaster Recovery Plans (IDRP) that are designed to achieve the RTO (Recovery Time Objective) of the applications that rely on these services.

Both Applications and Information Technology Infrastructure systems need to be designed to achieve availability targets required to sustain the business functions they support. See 9-9 of this document for Availability requirements.

Application and Infrastructure Service owners may use templates when developing DR plans.

12-3.2 Application Disaster Recovery Plan Requirements

The Application Disaster Recovery Plan (ADRP) Requirements are as follows:

a. Each application that is registered in the Enterprise Information Repository (EIR) must have an ADRP.

b. The requirements for the plan are determined based on the Criticality results of the Business Impact Assessment (BIA). See 3-2.3 of this document for requirements of Criticality determination. The ADRP must be designed to achieve the recovery time objectives (RTO) required to meet the business requirements as specified in the BIA.

c. The ADRP does not include the recovery plans for the infrastructure that it's depend upon.

d. The ADRP documentation is stored in the Technical Solution Life Cycle (TSLC) IT Artifact Library systems documentation testing section of the application as a Program-Level Artifacts and is considered "Sensitive".

e. The ADRP must be reviewed, tested, and the results certified by the development organization and the executive sponsor. Evidence of the testing and certification must be kept in the TSLC IT Artifact Library as

a Program-Level Artifacts and is considered "Sensitive". Test results are also recorded in the EIR system.

f. ADRP's Critical-High and Critical-Moderate applications must be tested within 180 days of the application going into production and within 180 days of changes which would invalidate previous tests.

g. Applications designated as Critical-High must be tested within 18 months of the last successful test.

h. Applications designated as Critical-Moderate must be tested within 36 months of the last successful test and within 12 months of changes which would invalidate previous tests.

i. Non-Critical (Low) applications are not required to conduct testing of their ADRP. As a result, the application may not be recovered in the event of a site outage. It is recommended that when the BIA is reviewed as required in 6-2 of Handbook AS-805A the criticality classification is carefully considered in light of an extended outage.

j. Failed tests must be re-attempted within 90 days of the failed test.

k. All recovery documents must be protected as restricted information.

12-3.3 Infrastructure Disaster Recovery Plan (IDRP)

Infrastructure Disaster Recovery Plan is an internal documented process or set of procedures to recover and protect the Postal Service IT Infrastructure in the event of a disaster as follows:

a. Many applications are dependent on shared information technology infrastructure services. Therefore these services must be designed to meet the availability requirements of the applications using the service. See 9-9 for availability requirements.

b. The IDRP must support the RTO for the most critical application that uses the Infrastructure Service.

c. The IDRP must be developed and certified by the Infrastructure Service Owner and the executive sponsor (see 2-2.11, Executive Sponsors).

d. The IDRP must be maintained in the designated plan repository. The availability to the repository must not be dependent on any one facility.

e. Infrastructure Services must have contingency plans that address the following:

(1) Loss of capacity due to failures of underlying requirements (power, cooling, facilities, servers, network, etc.).

(2) Loss of connectivity.

(3) Denial of Service attacks.

(4) Data corruption.

f. The IDRP must be exercised quarterly to insure DR infrastructure services provide the same functionality as production.

g. Test activities and results are documented as part of the normal change and configuration management services.

The IDRP must include essential personnel to support and validate recovery.

This page intentionally left blank

13 Security Incident Management

13-1 Policy

Postal Service information resources must be protected against events that may jeopardize information security by contaminating, damaging, or destroying information resources. The Postal Service requires that all information security incidents be immediately reported to CyberSafe regardless of whether damage appears to have been incurred.

Security incident management topics addressed in this chapter include the following:

a. Information security incident identification.

b. Incident prevention, reporting, response, and containment.

c. CyberSafe incident process and activities.

All personnel must adhere to the incident prevention, reporting, and containment standards to ensure adequate protection of Postal Service information resources.

13-2 Information Security Incident Identification

Information security incidents are events, whether suspected or proven, deliberate or inadvertent, that threaten the integrity, availability, or confidentiality of information resources. The reporting of incidents enables the responsible organizations to review the security controls and procedures; establish additional, appropriate corrective measures, if required; and reduce the likelihood of recurrence. To protect the Postal Service computing environment, the manager, Corporate Information Security Office (CISO), may become involved at any point on any level for information security-related incidents impacting the Postal Service.

Reportable incidents include, but are not limited to, the following:

a. Physical loss, theft, or unauthorized destruction of Postal Service information resources (e.g., missing or damaged hardware, software, or electronic media).

b. Unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information.

c. Internal or external unauthorized access attempts to access information or the facility where the information resides.

d. Unauthorized activity or transmissions using Postal Service information resources.

e. Internal or external intrusions or interference with Postal Service networks (e.g., denial-of-service attacks, unauthorized activity on restricted systems, unauthorized modification or deletion of files, or unauthorized attempts to control information resources).

f. Information resources with system software that is not patched to the current level.

g. Information resources with virus protection software that is not patched to the current level or is disabled.

h. Information resources with virus pattern recognition files that are not current.

i. Sudden unavailability of files or data normally accessible.

j. Unexpected processes (e.g., e-mail transmissions) that start without user input).

k. Files being modified when no changes in the files should have occurred.

l. Files appearing, disappearing, or undergoing significant and unexpected changes in size.

m. Systems displaying strange messages or mislabeled files or directories.

n. Systems becoming slow, unstable, or inaccessible (e.g., will not boot properly).

o. Data altered or destroyed or access denied outside of normal business procedures.

p. Detection of unauthorized personnel in controlled information security areas.

q. Security violation, suspicious actions, or suspicion or occurrence of embezzlement or other fraudulent activities.

r. Suspected bribery, kickbacks, and conflicts of interest.

s. Revenue loss involving an information system.

t. Prohibited mass electronic mailings.

u. Potentially dangerous activities or conditions.

v. Illegal activities.

w. Violation of Postal Service information security policies and procedures.

x. Identity theft.

y. Detection of unauthorized wireless access points.

13-3 Incident Prevention, Reporting, Response, and Containment

13-3.1 Incident Prevention

The following actions by Postal Service personnel can help prevent information security incidents:

a. Display proper badge when in any Postal Service facility.

b. Be aware of your physical surroundings, including weaknesses in physical security and the presence of any unauthorized visitor.

c. Use only approved computer hardware and software with the latest patches installed.

d. Use updated virus protection software and pattern recognition files.

e. Do not download, install, or run a program unless you know it to be authored by a person or company that you trust.

f. Use a personal firewall.

g. Use a strong password of at least eight characters composed of upper- and lower-case alphabetic, numeric, and special characters.

h. Encrypt sensitive-enhanced and sensitive information physically removed from a Postal Service facility.

i. Encrypt sensitive-enhanced and sensitive information in transit.

j. Back up data stored on local workstation and physically secure the backup copies.

k. Be wary of unexpected attachments. Know the source of the attachment before opening it. Remember that many viruses originate from a familiar e-mail address.

l. Be wary of URLs in e-mail or instant messages. A common social engineering technique known as phishing uses misleading URLs to entice users to visit malicious Web sites. URLs can link to malicious content that, in some cases, may be executed without your intervention.

m. Be wary of social engineering attempts to solicit sensitive-enhanced or sensitive information (e.g., account numbers and passwords).

n. Users of technology such as instant messaging and file-sharing services should be careful of following links or running software sent by other users.

13-3.2 Incident Reporting

Information security incidents must be immediately reported to CyberSafe via telephone at 1-800-USPS-HELP or via an e-mail to *CyberSafe@usps.gov.* The CyberSafe telephone number is a 24 X 7 hotline. Do not dismiss a suspected incident or discount its seriousness.

In addition to CyberSafe, the following personnel may be notified, as appropriate:

a. Help Desk at 1-800-USPS-HELP or 1-800-877-7435.

b. Immediate supervisor or manager.

c. Local system administrator or local technical support.

d. Security control officer (SCO).

e. Inspection Service at 1-877-876-2455.

f. Office of the Inspector General (OIG) at 1-888-877-7644.

A PS Form 1360, *Information Security Incident Report,* must be completed and submitted to CyberSafe. An acceptable facsimile with the same information required on the form may be submitted.

13-3.3 Incident Response

Information security situations and incidents must be handled in a way that minimizes damage, reduces recovery time and costs, and mitigates the risks to our customers and personnel. CyberSafe coordinates responses to information security situations and incidents.

13-3.4 Incident Containment

When an information security-related situation or incident is suspected or discovered, personnel must take steps, as directed by CyberSafe, to protect the information resource(s) at risk. Appropriate actions are the following:

a. Do not shut down or power off a system after a computer incident occurs. All suspect systems and devices that are already powered down should remain in that state.

b. Do not make any changes to the equipment or network in question without direction from CyberSafe.

c. Do not discuss or e-mail anyone about the situation or incident unless directed to do so by CyberSafe.

d. Follow CyberSafe instructions with regard to options and strategies for containment and recovery from the incident.

e. Close and lock doors to protect unattended equipment.

f. Do not touch the keyboard. Take a photograph of the screen or make a note of the information displayed before turning off the computer monitor so the screen cannot be viewed.

g. Challenge personnel without badges.

Supervisors or managers who suspect, discover, or are notified of a security-related event must initiate the following response procedures to contain the incident, protect the confidentiality and integrity of Postal Service information, and ensure business continuity:

a. Notify CyberSafe for assistance to contain, eradicate, and recover from the security incident.

b. Notify the Inspection Service of a physical security incident.

c. Document in a journal or log all conversations and actions taken during the incident handling and response process and make this log available to management personnel on request.

d. Ensure personnel follow contingency plans for recovering from disruptive incidents.

e. Ensure the completion of a PS Form 1360.

13-3.5 Mass Data Compromise Plan

Implement a Mass Data Compromise Plan (MDCP) to provide a strategy for addressing the dynamics of a critical incident. A critical incident is one that threatens confidentiality, integrity or availability of Postal Service information assets with high impact, high threat involving high risk and great vulnerability. The MDCP defines the roles and responsibilities for critical incident response team members, defines critical incident severity levels, outlines a process flow for critical incident management, and includes methodologies for conducting response activities.

13-4 CyberSafe Incident Process and Activities

13-4.1 Preliminary CyberSafe Activities

The following preliminary activities can improve CyberSafe's ability to respond to information security incidents:

a. Develop an incident response plan. Predetermine necessary actions and responses to specific classes of incidents to facilitate making decisions under pressure with minimal information.

b. Implement secure connections to make intrusion detection system (IDS) policy changes and attack signature updates.

c. Verify automated responses from IDS.

d. Conduct penetration testing at times known only to personnel with a need to know.

e. Regularly review available information sources (e.g., advisories and research findings) to maintain currency.

f. Notify management of potentially harmful events.

g. Prioritize the severity of information security incidents.

h. Document lessons learned to improve CyberSafe operations.

13-4.2 CyberSafe Incident Process

13-4.2.1 Incident Categorization

Incidents must be categorized based on severity and associated response times. The severity of the incident will determine the appropriate notification process and escalation procedure. Incident severity levels and response times are defined as follows (per the Postal Service CyberSafe severity code procedures):

a. Severity 1 — National Impact: Incidents with the greatest negative impact on the Postal Service. Severity level 1 is assigned when an incident has national impact or when multiple systems or sites are down or seriously affected.

b. Severity 2— Site Impact: Incidents impacting a major IT or field site or local area network (LAN) segment.

c. Severity 3 — Customer Impact: Incidents impacting one or more workstations, employees, contractors, or customers.

d. Severity 4 — Minimal Impact: Incidents with minimal or no impact.

13-4.2.2 Processing Incidents Reports

CyberSafe is responsible for the following:

a. Categorizing incidents.

b. Protecting the confidentiality of information contained in the incident report and subsequent information identified in the analysis.

c. Ensuring legal issues, requirements, and restraints caused by criminal and civil investigations are appropriated addressed.

d. Logging and tracking security incident reports.

e. Monitoring incidents to ensure appropriate response and immediate resolution of security incidents.

f. Engaging appropriate organizational resources (e.g., virus response team, OIG, and Inspection Service).

g. Notifying the CPO and responsible functional VP (data steward) of any suspected breaches involving sensitive or sensitive-enhanced information.

h. Evaluating and escalating incident reports requiring further action.

i. Retaining incident reports, supporting evidence, and journals for 1 year or for a time period determined by the OIG.

j. Providing Inspection Service and OIG access to all reported information security incidents.

k. Complying with federal sector security incident reporting requirements.

13-4.2.3 Incident Investigation

A member of the OIG-CCU team is co-resident with CyberSafe and investigates, along with the Inspection Service, violations of state and federal laws enacted to protect the authenticity, privacy, integrity, and availability of electronically stored and transmitted information.

13-4.2.4 Incident Analysis

CyberSafe analyzes security incidents and prepares reports summarizing the causes, frequency, and damage assessments of information security incidents.

CyberSafe management analyzes CyberSafe reports to improve the information security program and keep Postal Service executive management apprised on the state of information security.

13-4.2.5 Incident Escalation

It may be necessary to escalate an individual incident up the management chain based on the following criteria:

a. Number of sites and systems under attack.

b. Type of data at risk.

c. Severity of the attack.

d. State of the attack.

e. Source or target of the attack.

f. Impact on the integrity of the infrastructure or cost of recovery.

g. Attack on a seemingly "secure" information resource.

h. Personnel awareness of the attack.

i. New attack method use.

13-4.2.6 Incident Closure

Before an incident is closed the incident must be categorized; the root cause must be determined; damage must be assessed and reported to management and one or more of the national CyberSafe if required; and the incident's closure confirmed with the initiator.

14 Security Compliance and Monitoring

14-1 Policy

All Postal Service information resources are the property of the Postal Service. The Postal Service has the legal right to monitor and audit the use of its information resources as necessary for compliance with policies, processes, procedures, and standards to ensure the appropriate use and protection of Postal Service information resources.

The activities of all Postal Service personnel who use Postal Service computing resources may be subject to audit or monitoring, and any detected misuse of Postal Service computing resources may be subject to disciplinary action up to and including removal, termination, and criminal prosecution.

Security topics addressed in this chapter include the following:

a. Compliance.

b. Monitoring.

c. Audits.

d. Confiscation and removal of information resources.

This monitoring policy does not apply to Postal Service customers who visit the Postal Service Web site (i.e., no attempt is made to identify individual customers or their usage habits). See the Postal Service Privacy Policy on http://www.usps.com for additional information.

14-2 Compliance

The Postal Service exercises due care in ensuring all personnel and contractors working on its behalf are in compliance with information security policies and associated standards and procedures as defined by the Postal Service. Additionally, the Postal Service monitors, reviews, and properly mitigates all instances of noncompliance throughout the organization using processes that include, but are not limited to, the following:

a. Regular testing of security systems and processes.

b. Vulnerability scans.

c. Inspections, reviews, and evaluations.

d. Monitoring.

e. Audits.

f. Confiscation and removal of information resources.

g. Information security compliance training.

The importance of compliance with government and industry regulations and standards is to prevent data breaches, loss of reputation and customers, fines and lawsuits.

14-2.1 Regular Testing of Security Systems and Processes

Systems, processes, and custom software must be tested regularly because hackers and others continually discover vulnerabilities introduced in new software inadvertently by employees, contractors, and business partners. How testing is conducted is described in Exhibit 14-2.1.

Security testing must replicate real world attacks to [1] determine the effectiveness of preventive controls and if critical assets are exposed and [2] to provide insight into the actual risk posture of the information resource and highlight trends.

Exhibit 14-2.1

Regular Testing of Security Systems and Processes

Frequency	Testing Activities
Continuously	Monitor all network traffic and alert personnel to suspected compromises using network intrusion-detection systems, host-based intrusion detection systems, and intrusion prevention systems.
Weekly	Use file integrity monitoring software to alert personnel when files have been modified without authorization. Configure software so it can compare files.
Quarterly	Use a wireless analyzer to identify all wireless devices in use. Scan for vulnerabilities in internal and external networks (or when system components have been added, network topology has changed, firewall rules have been modified, or products have been updated).
Annually	Test security controls, limitations, network connections, and restrictions to identify unauthorized access attempts. Perform network-layer penetration testing (or when the infrastructure has been upgraded or modified (i.e., the operating system has been upgraded or a subnetwork or Web server has been added). Perform application-layer penetration testing (or when an application has been modified) to understand the intricate interactions and exploitable paths hidden in the code.
As Required	Whenever changes are made to the PCI environment. Whenever the Hardening Standards Team requests a hardening standards compliance check to ensure Postal Service hardening standards are being implemented.

The risks associated with newly discovered vulnerabilities must be documented and forwarded to the Corporate Information Security Office/ ISSO for inclusion into either the Risk Mitigation Plan for each system or Risk Register.

14-3

14-2.2 Vulnerability Scans

The Corporate Information Security Office Information Systems Security (CISO ISS) conducts vulnerability scans on applications, infrastructure components, and facilities. The vulnerability scan process identifies and assigns a risk ranking to security vulnerabilities based on industry best practices. For example, a "High" risk vulnerability will include a CVSS base score of 4.0 and above, and/or a vendor-supplied patch missing that is classified as "critical" and/or a vulnerability affecting a critical system component. The executive sponsor is responsible for coordinating the resolution of the vulnerabilities identified with the responsible organization (e.g., the manager IT Computer Operations for operating system and database software; the Business Relationship Management manager for application software, etc.).

14-2.3 Inspections, Reviews, and Evaluations

Inspections, reviews, and evaluations must be conducted for information resources and facilities to ensure compliance with Postal Service information security policies. A process is in place to monitor internal control compliance on an ongoing basis.

The CISO conducts inspections, reviews, and evaluations of information resources:

a. As part of the certification and accreditation (C&A) process.

b. When informally or formally requested by the supervisor or manager of an information resource.

c. At the discretion of the CISO or the VP IT Operations as necessary to evaluate the security of information resources.

The Inspection Service and/or CISO conducts inspections, reviews, and evaluations of Postal Service facilities.

14-2.4 Penetration Testing

The Corporate Information Security Office Cybersecurity Risk Penetration Testers conduct penetration testing on applications, infrastructure components, and facilities. Although USPS leaders and Information System managers are expected to engage in scheduled penetration testing engagements, such as those prescribed elsewhere within this document, CISO Risk reserves the right to perform penetration testing as needed throughout the organization.

Postal personnel are expected to provide assistance as directed by the needs of the penetration testers in the course of their assessment activities, to include disclosure of documentation and access to perform testing. Engagements may be performed as needed at the direction of the CISO and Cybersecurity Risk Managers to provide independent validation, assist in investigations, and to help audit processes and procedures throughout The Postal Service.

14-3 Monitoring

Monitoring is used to improve security for Postal Service information resources to ensure appropriate use of those resources and to protect Postal Service resources from attack. Use of Postal Service information resources constitutes permission to monitor that use. Nonbusiness (i.e., personal) information may be viewed when monitoring Postal Service information resources.

All personnel are advised that the information on Postal Service non-publicly available information resources may be monitored and viewed by appropriate, authorized personnel, regardless of privacy concerns. The Postal Service reserves the right to do the following:

a. Review the information contained in or traversing Postal Service information resources.

b. Review the activities on such information resources.

c. Act on information discovered as a result of monitoring and disclose this information to law enforcement and other organizations as deemed appropriate by Postal Service personnel.

14-3.1 What Is Monitored

Monitoring of Postal Service information resources may include, but is not limited to, the following:

a. Network traffic.

b. Application and data access.

c. Keystrokes and user commands.

d. E-mail and Internet usage.

e. Message and data content.

f. Unauthorized access points.

14-3.2 User Agreement to Monitoring

Any use of Postal Service information resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of Postal Service information resources:

a. Agree to comply with Postal Service policy concerning the use of information resources.

b. Acknowledge that their activities may be subject to monitoring.

c. Acknowledge that any detected misuse of Postal Service information resources may be subject to disciplinary action and prosecution pursuant to the United States Criminal Code (Title 18 U.S.C. § 1030).

14-3.3 User Monitoring Notification

Where possible, users are notified by the display of an authorized Postal Service warning banner (see Exhibit 14-3.3) that the information on Postal Service networks and workstations may be monitored and viewed by authorized personnel, regardless of privacy concerns.

The Postal Service-authorized warning banner must be displayed to users prior to granting session access to Postal Service information resources and be included in information security awareness training. The legal authority and obligations as indicated in the warning banner will apply throughout the entire session users have on the Postal Service information resources.

Applications that are single sign-on (SSO) or single log-on (SLO) compliant are not required to display an additional warning banner page as long as the executive sponsor can guarantee the user will see a warning banner at login for the session. Applications that are not SSO or SLO compliant must display a warning banner page.

Internal warning banners are not intended for display on Postal Service externally facing Internet Web sites where the Postal Service Internet Privacy Policy applies.

At a minimum, the warning banner must accomplish the following:

a. Identify the computer system as a Postal Service computer system protected by the United States Criminal Code.

b. Provide notification of monitoring.

c. Be followed by a pause requiring manual intervention to continue.

d. Identify the information resource as a Postal Service information resource and alert users that they have no expectation of privacy.

e. Warn users that activities may be monitored and that unauthorized access is prosecutable pursuant to the United States Criminal Code (Title 18 U.S.C. § 1030).

Note: Deviations from the authorized standard warning banner are not allowed unless approved in writing by the manager, CISO.

Exhibit 14-3.3
Authorized Standard Postal Service Warning Banner

WARNING! FOR OFFICIAL USE ONLY...

This is a U.S. Government computer system or mobile device and is intended for official and other authorized use only. Unauthorized access or use of this system or mobile device may subject violators to administrative action, civil, and/or criminal prosecution under the United States Criminal Code (Title 18 U.S.C. § 1030).

All information on this computer system or mobile device to include GPS location services may be monitored, intercepted, recorded, read, copied, captured, and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy using this system or mobile device. Any authorized or unauthorized use of this computer system or mobile device signifies consent to and compliance with Postal Service policies and these terms.

I agree.

14-3.4 Requesting User Monitoring

Requests for monitoring network traffic, application and data access, keystrokes and user commands, and e-mail and Internet usage must be in writing and directed to the manager, CISO.

Requests for monitoring message data content or Internet usage must be in writing and directed to the chief privacy officer (CPO).

14-3.5 Approving User Monitoring

The manager, CISO, has the responsibility to authorize in writing monitoring or scanning activities for network traffic, application and data access, keystrokes and user commands, and e-mail and Internet usage for Postal Service infrastructure or information resources. Personnel (except the Inspection Service and OIG) must receive authorization from the CISO prior to conducting monitoring and scanning activities.

The CPO has the responsibility to authorize, in writing, requests for message data content, or Internet usage monitoring. The Information Catalog Program (ICP) Office is responsible for documenting and servicing the request.

In case of threats to the Postal Service infrastructure, network, or operations, the manager, CISO, is authorized to take appropriate action, which may include viewing and/or disclosing data to protect Postal Service resources or the nation's communications infrastructure.

14-3.6 Infrastructure Monitoring

The manager, CISO, is responsible for ensuring the security of the Postal Service infrastructure through the following:

a. Providing security incident detection through perimeter virus scanning, intrusion-detection services, and security event correlation tools.

b. Performing network, Web, host, application, and database vulnerability analyses.

c. Performing data loss prevention analyses to prevent sensitive and sensitive-enhanced information from leaving the protected environment.

d. Performing data at rest searches for unprotected sensitive and sensitive-enhanced information.

e. Monitoring the Postal Service infrastructure, investigating incidents, and resolving or reassigning incidents immediately to the appropriate group for action.

f. Monitoring system-level audit logging.

g. Monitoring PCI service providers for compliance with the current PCI DSS.

14-3.7 Intrusion Detection

Intrusion-detection devices are implemented to monitor the infrastructure. The use of all monitoring devices, except those used by the OIG, must be approved by the manager, CISO ISS. Unauthorized installation and use of monitoring devices are strictly prohibited.

14-3.8 Data Loss Protection Program

The Data Loss Protection (DLP) program was implemented to protect sensitive and proprietary information entrusted to the Postal Service by its employees, customers, contractors, and vendors (suppliers). The DLP program supports Postal Service compliance with the Privacy Act, the PCI industry, many state identity theft notification laws, the Gramm-Leach-Bliley (GLB) Act, and the Sarbanes Oxley (SOX) Act. The software-based solution uses business rules to analyze the contents of all outbound electronic communications including email, web mail, file transfers, other web-based (HTTP) messages to look for sensitive information. The current business rules look for the existence of credit card numbers and social security numbers being transmitted in clear text. When sensitive information is found, the message is flagged for further analysis by CISO.

14-3.9 Continuous Monitoring Guidelines

To ensure compliance with information security policies, the Postal Service must regularly assess its information security readiness and implement

solutions that mitigate vulnerabilities, misconfigurations, and prevent unnecessary exposures by providing real-time visibility and control over servers, desktops, laptops, notebooks, and other mobile devices.

Given that threats are constantly evolving, the Postal Service must monitor critical assets more frequently so they can detect if something illegal or unauthorized has occurred and respond quickly to minimize the damage.

The most important actions/assets to monitor continuously are the ones that are most volatile (e.g., new versions of software and new hardware) and the ones the attackers are exploiting. The Consensus Audit Guidelines (were developed to address the continuous monitoring requirements delineated in National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

The Consensus Audit Guidelines recommended frequencies for meeting the requirement for continuous monitoring are:

a. Test the computing environment, including servers and workstations, three times a day.

b. Check for vulnerabilities at least once a week.

c. Check configuration settings no less than once every 15 days.

For example, the Department of Homeland Security Continuous Diagnostics and Mitigation program goal is to scan critical systems every 20 minutes (all systems every 1 to 3 days), collect results, triage and analyze results, and fix the worst problems first.

The Postal Service must understand the day-to-day operational status of controls deployed and how those controls are standing up to cyber threats.

Areas of focus must be hardware and software asset management, configuration settings, account and privilegé management, ports/protocols/ services for infrastructure devices, local computing environment events, network and infrastructure events, and enclave events.

14-4 Audits

14-4.1 Conducting Audits

The OIG has the authority to conduct audits, investigations, and evaluations of Postal Service programs and operations to ensure the efficiency and integrity of the Postal Service. The OIG coordinates investigative audits through the manager, CISO. Audits associated with financials [e.g., year-end audits and Sarbanes-Oxley Act (SOX) audits] are coordinated through the SOX Program Management Office.

14-4.2 Responding to Audits

Corporate management responsible for the audited information resource must respond to internal and external audit findings and ensure that the information resources under their control comply with Postal Service information security policies and procedures.

14-4.3 Audit Guidelines

The following critical information security controls identified in the CAG represent the highest-priority defenses that the Postal Service should focus on, based on the likelihood of real-world attacks:

a. Inventory of authorized and unauthorized devices.

b. Inventory of authorized and unauthorized software.

c. Secure configurations for hardware and software on laptops, workstations, and servers.

d. Secure configurations for network devices including firewalls, routers, and switches.

e. Boundary defense.

f. Maintenance, monitoring, and analysis of security audit logs.

g. Application software security.

h. Controlled use of administrative privileges.

i. Controlled access based on need to know.

j. Continuous vulnerability assessment and remediation.

k. Account monitoring and control.

l. Malware defenses.

m. Limitation and control of network ports, protocols, and services.

n. Wireless device control.

o. Data loss prevention.

p. Secure network engineering.

q. Penetration tests.

r. Incident response capability.

s. Data recovery capability.

t. Security skills assessment and appropriate training to fill gaps.

14-5 Confiscation and Removal of Information Resources

The CISO, OIG, Inspection Service, or their designee may confiscate and remove any information resource suspected to be the object of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be used in forensic analysis of a security incident. The CISO, OIG, Inspection Service, or their designee, as appropriate, must verify that the chain of evidence (associated with the possession of the confiscated information resource) is preserved and documented.

1 Introduction: Corporate Information Security

1-1 Purpose

The Postal Service™ is committed to creating and maintaining an environment that protects Postal Service information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. Information resources are strategic assets vital to the business performance of the Postal Service. Refer to Exhibit 1-7 for examples of information resources. Information resources are also protected by law and governed by law. Handbook AS-805, *Information Security,* establishes an organization-wide standardized framework of information security policies to ensure the detection, prevention, response to, and investigation of cybercrime incidents and misuse of Postal Service information technology assets. Adherence to information security policies will safeguard the integrity, confidentiality, and availability of Postal Service information and protect the interests of its personnel, business partners, and the public.

Adherence to information security policies enables compliance with regulations to which the Postal Service is subject, including Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standards (PCI-DSS). This policy reflects standards and guidelines suggested by industry organizations such as the Public Company Accounting Oversight Board (PCAOB), American Institute of Certified Public Accountants (AICPA), Committee of Sponsoring Organizations (COSO), and National Institute of Standards and Technology (NIST).

Information security policy will ensure the creation and implementation of an environment that:

a. Protects information resources critical to the Postal Service.

b. Protects information as mandated by federal laws, regulations, directives, law enforcement and judicial processes, and industry requirements.

c. Protects the personal information and privacy of employees and customers.

d. Reinforces the reputation of the Postal Service as an institution deserving of public trust.

e. Complies with due diligence standards for the protection of information resources.

f. Assigns responsibilities to relevant Postal Service officers, executives, managers, employees, contractors, partners, and vendors.

g. Reviews and revises information security policies and procedures in accordance with evolving security threats.

The following principles guide the development and implementation of Postal Service information security policies and practices:

a. Information is:

- A critical asset that must be protected.
- Restricted to authorized personnel for authorized use.

b. Information security is:

- Cornerstone of maintaining public trust.
- A business issue — not a technology issue.
- Risk based and cost effective.
- Aligned with Postal Service priorities, industry-prudent practices, government requirements, and federal laws.
- Directed by policy but implemented by business owners.
- Everybody's business.

1-2 Scope

Information resources are strategic assets vital to the business performance of the Postal Service. These strategic assets belong to the Postal Service as an organization and not to any individual or group of individuals and must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Postal Service's ability to conduct its mission.

Information security applies to all information resources, organizations, and personnel. Chapter 1 addresses the following:

a. Infrastructure components/systems.

b. Information resources.

c. Organizations and personnel.

d. Importance of compliance.

e. Policy exception and review.

1-3 Policy

The Postal Service information security policies are grouped in the following areas:

a. Security roles and responsibilities.

b. Information designation and control.

c. Security risk management.

d. Acceptable use.

e. Personnel security.

f. Physical and environmental security.

g. Development and operations security.

h. Information security services.

i. Hardware and software security.

j. Corporate network security.

k. Business continuity management.

l. Security incident management.

m. Security compliance and monitoring.

Information about individuals that is collected and stored by information resources is subject to the Privacy Act of 1974, as amended (Privacy Act).

The Privacy Act requires all federal agencies, including the Postal Service, to adhere to a minimum set of standards for the collection and storage of certain personal data and limits the disclosure of such Privacy Act information. Agencies are required to establish appropriate administrative, technical, and physical safeguards to protect Privacy Act data. These safeguards ensure the integrity and confidentiality of information resources containing Privacy Act data and protect against unauthorized disclosure of such data, which could result in substantial harm, embarrassment, unfairness, or inconvenience to an individual.

1-4 Supporting Documentation

The following handbooks, management instructions, and contract clauses provide implementation policy and guidelines for this handbook:

a. Handbook AS-805-A, *Information Resource Certification and Accreditation Process.*

b. Handbook AS-805-D, *Information Security Network Connectivity Process.*

c. Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment (MPE/MHE).*

d. Handbook AS-805-H, *Cloud Security.*

e. Management Instruction FM 640-2011-3, *Payment Card Industry Data Security Standard (PCI DSS).*

f. Contract clauses 1-1, Privacy Protection, and 4-19, Information Security Requirements in the Postal Service's *Supplying Principles and Practices.*

1-5 Policy Owner

The policy owner of this handbook is the manager of the Corporate Information Security Office.

1-6 Infrastructure Components/Systems

1-6.1 General

Infrastructure components/systems are the underlying foundation for information resources and include cyber-based resources (e.g., network hardware and software).

The infrastructure components/systems are usually major groupings or network segments that provide reusable and repeatable services for application systems and are generally considered to be critical components/ systems of the Postal Service computing environment.

An infrastructure component/system typically does the following:

a. The system is typically an underlying part of the Postal Service network environment.

b. The system does not provide a direct user interface and multiple user functionality.

c. The system provides reusable and repeatable services for multiple applications.

d. The system does not typically require periodic code changes or customer acceptance testing, developer intervention or regular upgrades.

1-6.2 External Technology Solutions

External technology solution types are categorized as follows:

a. Service-based contract solution.

b. Hosted solution.

c. Cloud solution.

1-6.2.1 Service-Based Contract Solution

A service-based contract solution is required for a company that is providing a service to the Postal Service such as financial services (Wells Fargo), Licensee (NCOA Link, Stamp reseller), and Inter-Agency Agreements. A service-based contract is different from other external technology solutions in that the service provider has custody of USPS data and is responsible for:

a. Protecting Postal Service data.

b. All aspects of its security (e.g., physical, personnel, network, application).

c. Mitigating and reporting incidents such as breaches.

1-6.2.2 Hosted Solution

A hosted solution requires the business partner to host a separate instance of an application for Postal Service use. The business partner typically owns or leases the physical servers used in the solution and the servers utilized for Postal Service are not shared with anyone else. Data storage and backup requires segregation through encryption and physical or logical isolation/ separation based on data classification.

1-6.2.3 Cloud Solution

A cloud solution enables network access to a shared pool of configurable virtualized computing resources (e.g., networks, servers, storage, applications, and services) in which information technology enabled capabilities are delivered "as a service" to multiple customers using the same computing resources. The cloud environment can be rapidly scaled up or down and tailored to serve multiple consumers on demand with minimal management effort or service provider interaction.

Cloud solutions must not be confused with [1] hosted solutions that are managed and maintained by the supplier and provide physical separation of the hardware that is leased, purchased or isolated for the exclusive use of Postal Service or [2] service-based contracts where the supplier takes ownership and full responsibility for the security of the data.

Data must not be viewed, processed, transmitted, or stored outside the United States (including U.S. territories). See Handbook AS-805-H for additional cloud security requirements.

1-6.3 External Technology Solution Security and Privacy Assessments

1-6.3.1 Service-Based Contract Solution Security and Privacy Assessment

To determine how the service provider will protect Postal Service data, all service-based contract solutions must be evaluated by Corporate Information Security (CISO) and the Privacy Office to evaluate the service provider's protection posture. This evaluation will include, but is not limited to a review of the service provider's internal documentation as well any third-party assessment documentation that can assist in verifying third-party control implementation, such as, ISO 27001, SOC2, PCI DSS, NIST/FedRAMP.

1-6.3.2 Cloud and Hosted Solution Security and Privacy Assessment

To determine how the solution provider will protect Postal Service data:

a. The offsite hosting letter must be reviewed and approved by CISO and Privacy Office.

b. All hosted and cloud solutions must complete the USPS Certification and Accreditation process.

1-6.3.3 Cloud Solution Security and Privacy Assessment

All cloud solutions collecting, transmitting, or storing sensitive or sensitive-enhanced (including PII, PCI, and law enforcement) data must complete and maintain a current FedRAMP Authorization as guided by the AS 805H.

Unless otherwise stated in the contract with the CSP, a security assessment will be conducted using the Postal Service Certification and Accreditation process.

All cloud solutions regardless of sensitivity and criticality, will utilize the Postal Service Certification and Accreditation process to evaluate the risk regardless of the FedRAMP status. If the solution has been FedRAMP evaluated, CISO will assess that evaluation.

1-7 Information Resources

Information security policies apply to all information, in any form, related to Postal Service business activities, employees, or customers that have been created, acquired, or disseminated using Postal Service resources, brand, or funding. Information security policies apply to all technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information. Information security policies also apply to all information systems, infrastructure, applications, products, services, telecommunications networks, computer-controlled mail processing equipment, and related resources, which are sponsored by, operated on behalf of, or developed for the benefit of the Postal Service.

Exhibit 1-7 shows examples of information technologies and the information they contain that are collectively known as information resources. Information resources may be referred to as technology solutions within the Technical Solutions Life Cycle (TSLC).

Exhibit 1-7
Examples of Information Resources

Category	Description	Examples
Systems and Equipment	All multi-user computers and computer controlled systems and their components.	■ Data Processing ■ Automated Information Systems (AIS) ■ Process Control Computers ■ Process Control Systems ■ Embedded Computer Systems ■ Mainframe Computers ■ Minicomputers ■ Microcomputers ■ Microprocessors ■ Office Automation Systems ■ Stand-Alone, Shared Logic, or Shared Resource Systems ■ Firmware ■ Servers ■ Kiosks ■ Intelligent Vending Machines

Mail Processing Equipment (MPE)	All computer-controlled equipment and networks used in processing, distributing, and transporting the mail.	■ Bar Code Sorters ■ Flat Sorters ■ Optical Character Readers ■ Data Collection System ■ Routers and Switches ■ Tray Management System ■ Forwarding Control System ■ MPE Support System

Category	Description	Examples
Single-User Computer Equipment	All computers and their components used by individuals.	■ Personal Computers (PCs) ■ Workstations ■ Mobile Computing Devices – Laptop Computers – Notebook Computers – Tablet Devices – Phablets – Handheld Computers – Smart Phones – Scanners
Hardware	All major items of equipment or their components associated with a computer system.	■ Central Processing Units (CPUs) ■ Random Access Memory (RAM) ■ Hard Drives ■ Network Interface Cards ■ Terminals ■ Monitors ■ Speakers ■ Video Display Terminals ■ Projection Equipment ■ Modems ■ Printers ■ Scanners
Software	All programs, scripts, applications, operating systems, HTML, and related resources.	■ Operating Systems (OS) ■ Programs (Source and Object) ■ Applications ■ Applets ■ Macros, Scripts ■ Database Management Systems ■ Custom Code ■ Associated Documentation
Data and Information	All information or data stored in digital format, or as a printed product of data stored in digital format.	■ Text Files ■ Documents ■ Spreadsheets ■ Digital Images ■ Electronic Mail ■ Tables ■ Databases ■ Biometrics Information

Products and Services	All objects, processes, functions, and information delivered by, for, or under the brand of the Postal Service.	■ Information Delivery Services ■ E-Commerce Applications ■ Digital Certificate Services ■ Web Site Content ■ Managed Services

Category	Description	Examples
Network Facilities	All communications lines and associated interconnected communications equipment.	■ Transition Lines ■ Terminal Equipment ■ Routers ■ Firewalls ■ Hubs ■ Switches ■ Local Area Networks (LANs) ■ Wide Area Networks (WANs) ■ Virtual Private Networks (VPNs) ■ Infrastructure ■ Internet ■ Intranet ■ Extranet ■ Telephone and Telephone Systems ■ Voice-Messaging Systems ■ Fax Machines ■ Videoconferencing Equipment ■ Wireless Communications
Media	All electronic and non-electronic media used for information exchange.	■ Magnetic Tapes ■ Magnetic or Optical Disks ■ Diskettes ■ USB Devices ■ Hard-Copy Printouts

1-8 Organizations and Personnel

Information security policies apply to all Postal Service functional organizations and personnel, including Postal Service employees, contractors, vendors, suppliers, business partners, and any other authorized users of Postal Service information systems, applications, telecommunication networks, data, and related resources, regardless of location. Information security applies to the Office of the Inspector General and the Inspection Service except where statutory authority exempts them.

For the purposes of these policies, the above entities are collectively known as personnel. This definition of "personnel" excludes customers whose only access is through publicly available services, such as public Web sites of the Postal Service.

These policies do not change the rights or responsibilities of either management or the unions pursuant to Articles 17 and 31 of the various

collective bargaining agreements or the National Labor Relations Act, as amended. These revisions do not bar the unions from using their own portable devices and media for processing information that is relevant for collective bargaining and/or grievance processing, including information provided by management pursuant to Articles 17 and 31 of the collective bargaining agreement or the National Labor Relations Act. There is no change to policy concerning restricted access to the Postal Service Intranet.

Note: For specific guidance regarding practices or actions not explicitly covered by these policies, contact the manager, Corporate Information Security Office, prior to engaging in such activities.

1-9 Importance of Compliance

1-9.1 Maintaining Public Trust

The public entrusts vast amounts of information to the Postal Service every day — information that the Postal Service is required by law and good business practice to protect. Compliance with information security policies will help protect information resources and enhance the reputation of the Postal Service as deserving of public trust.

1-9.2 Continuing Business Operations

The Postal Service is committed to delivering superior customer service in an increasingly competitive marketplace through the effective use of technology, information, and automation. Compliance with information security policies will help ensure the continuous availability and integrity of the technological infrastructure that is critical to the Postal Service's ability to perform its mission.

1-9.3 Protecting Postal Service Investment

Postal Service information resources represent a sizable financial investment in technologies and in information that can never be replicated. These information resources are of paramount importance to the mission of the Postal Service and to the country and must be protected.

1-9.4 Abiding by Federal Regulations

Postal Service information security policies are designed to respond to the intent and spirit of government laws, regulations, and directives.

1-10 Policy Exception and Review

1-10.1 Granting an Exception to the Policies

Any exception to the policies in this handbook must be based on a completed risk assessment and documented in a risk acceptance letter approved by the vice president, Information Technology, and the vice president of the function business area. (Risk acceptance is defined in 4-6, Risk-Based Information Security Framework, of this handbook). If the exception impacts sensitive or sensitive-enhanced information, the Chief Privacy Officer (CPO) must also approve the exception. (Information categories and levels are defined in 3-2, Information Designation and Categorization, of this handbook).

1-10.2 Policy Review

Information security policy is reviewed on semiannual basis and updated as needed to reflect changes to business objectives, government, and industry requirements, and risks to the computing environment. A call for updates is sent to applicable Postal Service organizations. Comments, suggestions, and recommended changes are submitted to the Corporate Information Security Office (CISO).

Organizations can submit suggestions and recommended changes to CISO anytime throughout the year, as the need arises. All comments, suggestions, and recommended changes are reviewed by the CISO for possible inclusion in information security policy documents.

The CISO responds to the submitter with a summary of the action to be taken. Approved changes are packaged into a draft change document which is then vetted with Postal Service organizations. The CISO reviews all comments received from the vetting process against federal laws, regulations, directives, circulars, memoranda, and standards; industry standards and best practices; and Postal Service business needs. The finalized change document is submitted for signoff by the chief security officer and for publication on PolicyNet.

2 Security Roles and Responsibilities

2-1 Policy

Information security is the individual and collective responsibility of all Postal Service personnel, business partners, and other authorized users. Access to information resources is based on an individual's roles and responsibilities. Only authorized personnel are approved for access to Postal Service information resources.

All information technology managers are responsible for securing the Postal Service computing environment, which includes information resources and infrastructure, by implementing appropriate technical and operational security processes and practices that comply with Postal Service information security policies.

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for implementing information security policies. All officers and managers must ensure compliance with information security policies by organizations and information resources under their direction and provide the personnel, financial, and physical resources required to appropriately protect information resources.

All Postal Service personnel are responsible for complying with all Postal Service information security policies.

2-2 Consolidated Roles and Responsibilities

2-2.1 Chief Information Officer and Executive Vice President

The chief information officer (CIO) and executive vice president is responsible for the following:

a. Acting as the senior information technology (IT) decision maker and corporate change agent to securely integrate the key components of business transformation: technology, processes, and people.

b. Providing advice and assistance to senior managers on information security policy and their compliance-based performance.

c. Promoting the implementation of an information security architecture to mitigate information security-related risk.

d. Promoting the protection of corporate information resources across Postal Service organizations and business partners.

e. Together with the vice president of the functional business area (data steward) and chief privacy officer (CPO), approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. If this responsibility is delegated, notice to that effect must be writing. See 3-5.5.

2-2.2 Chief Postal Inspector

The chief postal inspector is responsible for the following:

a. Establishing policies, procedures, standards, and requirements for personnel, physical, and environmental security.

b. Approving the identification of sensitive positions.

c. Conducting background investigations and granting personnel clearances.

d. Conducting site security reviews, surveys, and investigations of facilities containing Postal Service computer and telecommunications equipment to evaluate all aspects of physical, environmental, and personnel security.

e. Providing technical guidance on physical and environmental security activities that support information security, such as controlled areas, access lists, physical access control systems, and identification badges; providing protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

f. Providing security consultation and guidance during system, application, and product development to assure that security concerns are addressed and information and/or evidence that may be needed for an investigation is retained by the information resource.

g. Assisting the manager, Corporate Information Security Office (CISO), with reviews, as appropriate.

h. Investigating reported security incidents and violations.

i. Conducting revenue/financial investigations including theft, embezzlement, or fraudulent activity.

j. Providing physical protection and containment assistance and investigating information security incidents as appropriate.

k. Funding CISO investigative efforts outside of those normally required.

l. Managing, securing, scanning, and monitoring the Inspection Service's network and information technology infrastructure.

m. Defining high-risk international destinations where personnel are prohibited from traveling with their standard issue Postal Service computers and communications equipment (including laptops, notebook computers, external hard drives, mobile devices, Universal Serial Bus (USB) devices, etc.).

n. Providing temporary equipment to use when traveling to high-risk international destinations.

2-2.3 Vice President, Information Technology

The vice president, Information Technology (IT), is responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of information processed by IT applications.

c. Ensuring compliance with the information security certification and accreditation processes.

d. Together with the vice president of the functional business area, accepting, in writing, residual risks of information resources under their control. The VP IT may delegate this authority to the applicable Business Relationship Management manager. If this authority is delegated, notice to that effect must be in writing.

e. Reporting to senior management on the status of an incident with a major IT application.

f. Defining and documenting secure coding best practices.

2-2.4 Manager, Computer Operations

The manager of Computer Operations is responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of information processed at IT sites.

c. Ensuring the protection and secure implementation of the Postal Service IT infrastructure.

d. Supporting the information security certification and accreditation processes.

e. Together with the vice president of the functional business area (data steward) and CPO, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from an IT facility. (If this responsibility is delegated, notice to that effect must be writing. See 3-5.5.)

f. Reporting to senior management on the status of an incident at a major
IT facility.

g. Reviewing and utilizing C&A documentation in the IT Artifacts Library.

h. Resolving identified vulnerabilities.

2-2.5 Chief Information Security Officer

The chief information security officer (CISO) is responsible for the following:

a. Setting the overall strategic and operational direction of the Postal Service information security program and the program's implementation strategies.

b. Engaging at any point on any level for issues related to information security that impact the Postal Service.

c. Recommending members to the Executive Cyber Risk Committee (ECRC).

d. Developing and disseminating information security policies, processes, standards, and procedures.

e. Managing the certification and accreditation (C&A) process.

f. Providing guidance on application security, reviewing the C&A documentation package, and accrediting sensitive-enhanced, sensitive, and critical information resources developed for, endorsed by, or operated on behalf of the Postal Service.

g. Managing the Network Change Review Board (NCRB) process.

h. Authorizing temporary access to information resource services.

i. Conducting site security reviews or providing support to the Postal Inspection Service during its site security reviews, as requested.

j. Providing consulting support for securing the network perimeter, infrastructure, integrity controls, asset inventory, identification, authentication, authorization, intrusion detection, penetration testing, and audit logs and for information security architecture, technologies, procedures, and controls.

k. Approving encryption technologies.

l. Providing leadership of the security initiatives for the Enterprise Architecture Forum.

m. Developing and implementing a comprehensive information security training and awareness program that is mandatory for all employees at time of hire and annually thereafter.

n. Serving as the central point of contact for all information security issues and providing overall consultation and advice on information security policies, processes, standards, procedures, requirements, controls, services, and issues.

o. At least semiannually, assessing the adequacy of information security policy and process to reflect changes to business objectives and the operating environment (including technology infrastructure, threats, vulnerabilities, and risks).

p. At least annually, assessing the adequacy of information security controls and recommending changes as necessary.

q. Establishing evaluation criteria and recommending security hardware, software, and audit tools.

r. Approving the establishment of shared accounts.

s. Ensuring compliance to information security policies and standards through inspections, reviews, and evaluations.

t. Providing support to the Office of the Inspector General (OIG) and the Inspection Service during the conduct of investigative activities concerning information security, the computing infrastructure, and network intrusions, as requested.

u. Providing support to the chief postal inspector during the conduct of facility/site security reviews, as requested.

v. Escalating security issues to executive management and promulgating security issues and recommended corrective actions across the Postal Service.

w. Authorizing monitoring and surveillance activities of information resources.

x. Authorizing (in case of threats to the Postal Service infrastructure, network, or operations) appropriate actions that may include viewing and/or disclosing data to protect Postal Service resources or the nation's communications infrastructure.

y. Confiscating and removing any information resource suspected of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be used in forensic analysis of a security incident.

z. Reviewing and approving information security policy for mail processing equipment/mail-handling equipment (MPE/MHE).

aa. Providing guidance and program direction for security solutions, and ensuring adherence of the solution to the existing policies.

2-2.6 Executive Cyber Risk Committee

The purpose of the Executive Cyber Risk Committee (ECRC) is to establish, communicate, and regularly review the USPS cyber risk capacity and appetite and keep the Postmaster General abreast of cyber risks that may impact the cyber network.

2-2.7 Vice Presidents, Functional Business Areas

The vice presidents of Postal Service functional business areas are responsible for the following:

a. Ensuring resources are available for completing information security tasks.

b. Ensuring the security of all information resources within their organization.

c. Together with the VP IT, accepting, in writing, residual risks of information resources under their control. The vice presidents of functional business areas may delegate this authority to the applicable executive sponsor. If this authority is delegated, notice to that effect must be in writing.

d. Ensuring that contractual agreements require all suppliers, contractors, vendors, and business partners under each VP's purview to adhere to Postal Service information security policies.

e. Together with the CIO and CPO, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. (If this responsibility is delegated, the delegation of responsibility must be writing.)

f. Oversee organizational compliance for regulatory and external requirements (SOX, PCI).

2-2.8 Vice President, Engineering

a. The vice president, Engineering Systems, is responsible for ensuring the security of information resources used in support of the MPE/MHE environment, including technology acquisition, development, and maintenance.

b. Oversee organizational compliance for regulatory and external requirements (SOX, PCI)

2-2.9 Vice President, Network Operations

The vice president, Network Operations, is responsible for the security of the mail and information resources used in support of strategies and logistics.

2-2.10 Officers and Managers

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for the following:

a. Implementing information security policies, ensuring compliance with information security policies by organizations and information resources under their direction, and invoking user sanctions as required.

b. Identifying sensitive information positions in their organizations and ensuring that personnel occupying sensitive positions hold the appropriate level of clearance.

c. Managing access authorizations and documenting information security responsibilities for all personnel under their supervision.

d. Ensuring all personnel under their supervision receive information security training commensurate with their responsibilities upon hire and annually thereafter, and maintaining auditable training records when there isn't an automated system.

e. Ensuring all personnel under their supervision comply with Postal Service information security policies and procedures.

f. Including employee information security performance in performance evaluations.

g. Supervising information security responsibilities of their onsite contractor personnel.

h. Processing departing personnel appropriately and notifying the appropriate system and database administrators when personnel no longer require access to information resources.

i. Initiating a written request for message data content or Internet usage monitoring and sending it to the CPO for approval.

j. Approving or denying requests, by personnel under their supervision, for access to information resources beyond temporary information resource services and reviewing those access authorizations on a semiannual basis.

k. Ensuring that all hardware and software are obtained in accordance with official Postal Service processes.

l. Protecting information resources and ensuring their availability through business continuity activities including plans, procedures, off-site backups, periodic testing, workarounds, and training/cross-training essential and alternate personnel.

m. Ensuring that personnel under their supervision who remove a portable electronic device or media from a Postal Service facility are aware of their responsibility for its security and have a place to secure the device or media when it is not being used.

n. Ensuring compliance with Postal Service information security policy and procedures.

o. Reporting suspected information security incidents to CyberSafe immediately, protecting information resources at risk during security incidents, containing the incident, and following continuity plans for disruptive incidents (see Chapter 13, Security Incident Management).

2-2.11 Executive Sponsors

Executive sponsors, as representatives of the vice president of the functional business area, are the business managers with oversight (e.g., funding, development, production, and maintenance) of the information resource and are responsible for the following:

a. Consulting with the CPO for determining information sensitivity and Privacy Act applicability.

b. Ensuring a business impact assessment (BIA) is conducted to determine the sensitivity and criticality of each information resource under his or her control and to determine the potential consequences of information resource unavailability.

c. Providing resources to ensure that security requirements are properly addressed and information resources are properly protected.

d. Ensuring completion of a site security review, if the facility hosts an information resource designated as sensitive-enhanced, sensitive, or critical.

e. Ensuring that contract personnel under their supervision comply with Postal Service information security policies and procedures.

f. Ensuring that all information security requirements are included in contracts and strategic alliances.

g. Ensuring compliance with and implementation of the Postal Service privacy policy; data collection, retention, and destruction policies; customer or employee privacy notices; and software licensing.

h. Appointing, in writing, an information systems security representative (ISSR).

i. Ensuring completion of security-related activities throughout the Information resource C&A life cycle.

j. Ensuring that information resources within their purview are capable of enforcing appropriate levels of information security services to ensure data integrity.

k. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.

l. Authorizing access to the information resources under their control and reviewing those access authorizations on a semiannual basis.

m. Maintaining an accurate inventory of Postal Service information resources and coordinating hardware and software upgrades.

n. Ensuring appropriate funding for proposed business partner connectivity, including costs associated with the continued support for the life of the connection.

o. Initiating and complying with the network connectivity request requirements and process as documented in the Information Security Network Connectivity Process.

p. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

q. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

r. Funding application recovery (including but not limited to hardware/ software licenses required, continuity plan development, testing, and maintenance) for applications.

s. If the VP functional business area delegated this authority to the executive sponsor, the executive sponsor will work jointly with the VP IT (or the Business Relationship Management manager if this authority is delegated) to review the C&A documentation package, accept the residual risk to an application, and approve the application for production or return the application to the applicable life cycle phase for rework.

t. Reporting suspected information security incidents to CyberSafe immediately, protecting information resources at risk during the security incident, containing the incident, and following continuity plans for disruptive incidents.

u. Coordinating the resolution of identified vulnerabilities with the appropriate IT organization (e.g., Computer Operations, Business

Relationship Management, Solutions Development and Support, etc.).

2-2.12 Functional System Coordinators

The functional system coordinator (FSC) role is an ad hoc activity assigned by a data steward and is not a position or job function. An FSC has expert knowledge of the information resource and is familiar with the people and levels of access being requested. The FSC role may be required for all information resources registered in eAccess/ARIS. The FSC role is restricted to authorized Postal Service employees and contractors.

An FSC is responsible for approving or denying a request based on the role or access level requested. If access to an information system is requested, the FSC is responsible for ensuring that the requestor has successfully completed the appropriate background investigation or obtained the appropriate clearance. The FSC has the last level of approval before a request is sent to the log-on administrator to create the account, which will then become active.

2-2.13 Business Relationship Management Portfolio Managers (formerly Portfolio Managers)

Business Relationship Management portfolio managers are responsible for the following:

a. Supporting the executive sponsor in the development of information resources and the C&A process, including the BIA, risk assessment, and business continuity plans.

b. If an ISSR has not been assigned by the executive sponsor, appointing an ISSR to perform security-related activities.

c. Providing coordination and support to executive sponsors and disaster recovery (DR) service providers for all matters relating to business continuity planning.

d. Reviewing the C&A documentation package and completing a risk mitigation plan for risks identified as high or medium. If a documented high or medium vulnerability will not be mitigated, preparing and signing a Risk Acceptance Letter as part of the C&A process.

e. Business Relationship Management portfolio managers are responsible for the following: If the VP IT delegated this authority to the Business Relationship Management portfolio manager, the Business Relationship Management portfolio managers will work jointly with the vice president of the functional business area (or the executive sponsor, if this authority is delegated) to review the C&A documentation package, accept the residual risk to an information resource, and approve the information resource for production or return the information resource to the applicable life-cycle phase for rework.

f. Ensuring that the information resource is registered in eAccess/ARIS.

g. Accepting personal accountability for adverse consequences if the information resource was placed in production before the C&A process was completed.

h. Managing projects through their project managers who are responsible for the following:

(1) Incorporating the appropriate security controls in all information resources.

(2) Developing and maintaining C&A documentation as required.

(3) Ensuring that the information resource is entered in the Enterprise Information Repository (EIR) and updated as required.

(4) Filing C&A documentation in the IT Artifacts Library and maintaining the hardcopies and electronic copies for the appropriate retention periods.

i. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

j. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

k. Completing along with their staff the annual C&A training.

l. Resolving identified vulnerabilities.

2-2.14 Managers of Information Technology Solution Centers

The managers of Information Technology Solution Centers are responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of data.

c. Ensuring the protection and secure implementation of the Postal Service IT infrastructure.

d. Ensuring compliance with the information security C&A processes.

e. Together with the vice president of the functional business area, accepting, in writing, residual risk of applications and approving deployment.

f. Together with the vice president of the functional business area, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. (If this responsibility is delegated, notice to that effect must be writing.)

g. Managing projects through their project managers who are responsible for the following:

(1) Incorporating the appropriate security controls in all information resources.

(2) Developing C&A documentation as required.

(3) Ensuring that the information resource is entered in the Enterprise Information Repository (EIR) and updated as required.

(4) Filing C&A documentation in the IT Artifacts Library and maintaining the hardcopies and electronic copies for the appropriate retention periods.

h. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

i. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

j. Functioning as the incident management team leader for their facility.

k. Identifying and training key technical personnel to provide support in business continuity planning for their facility, information resources housed in their facility, and the alternate DR facilities.

l. Resolving identified vulnerabilities.

2-2.15 Installation Heads

Installation heads are in charge of Postal Service facilities or organizations, such as areas, districts, Post Offices, mail processing facilities, parts depots, vehicle maintenance facilities, computer service centers, or other installations. Installation heads are responsible for the following:

a. Designating a security control officer (SCO) who is responsible for personnel and physical security at that facility, including the physical protection of computer systems, equipment, and information located therein.

b. Implementing physical and environmental security support for information security, such as the protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

c. Controlling physical access to the facility, including the establishment and implementation of controlled areas, access lists, physical access control systems, and identification badges.

d. Funding building security equipment and security-related building modifications.

e. Maintaining an accurate inventory of Postal Service information resources at their facilities and implementing appropriate hardware security and configuration management.

f. Maintaining and upgrading all security investigative equipment, as necessary.

g. Ensuring completion of a site security review, providing assistance to the Inspection Service and CISO as required, and accepting site residual risk.

h. Ensuring that the Postal Service security policy, standards, and procedures are followed in all activities related to information resources (including procurement, development, and operation) at their facility.

i. Ensuring that all employees who use or are associated with the information resources in the facility are provided information security training commensurate with their responsibilities and taking appropriate action in response to employees who violate established security policy or procedures.

j. Cooperating with the Inspection Service to ensure the physical protection of the network infrastructure located at the facility.

k. Developing, maintaining, and testing:

(1) Emergency Action Plans required for each facility to ensure personnel are safely evacuated and provides for the protection of the employees.

(2) Incident Management Facility Recovery Plan required for each major IT site.

(3) Workgroup Recovery Plan required for each business function.

(4) Disaster Recovery Plan (DRP) (business information systems disaster) documents required for each critical system that supports essential (core) business functions.

l. Implementing and managing the following plans and team members:

(1) Emergency Action Plan.

(2) Incident Management Facility Recovery Plan.

(3) Workgroup Recovery and "Beyond" Continuity of Operations (COOP) Plans.

(4) DRP (business information systems disaster) documents.

i. Reporting information security incidents to CyberSafe immediately, containing the incident, following continuity plans for disruptive incidents, and assessing damage caused by the incident.

j. Resolving identified vulnerabilities.

2-2.16 Chief Privacy Officer

The CPO is responsible for the following:

a. Developing policy for defining information sensitivity and determining information sensitivity designations.

b. Providing guidance on privacy issues to ensure Postal Service compliance with the Privacy Act, the Freedom of Information Act, Gramm-Leach-Bliley Act, and Children's Online Privacy Protection Act.

c. Developing privacy compliance standards, customer or employee privacy notices, and customer data collection standards, including cookies and Web-transfer notifications.

d. Developing appropriate data record retention, disposal, and release procedures and standards.

e. Approving requests for message data content or Internet usage monitoring.

f. Consulting on and reviewing the BIA and approving the determination of information sensitivity.

g. Providing guidance throughout the investigation of a mass data compromise relating to the privacy of customer and employee/ contractor personal information.

h. Developing communications to transmit to impacted parties to a mass data compromise.

2-2.17 Inspector General

The inspector general is responsible for the following:

a. Conducting independent financial audits and evaluation of the operation of the Postal Service to ensure that its assets and resources are fully protected.

b. Preventing, detecting, and reporting fraud, waste, and program abuse.

c. Investigating computer intrusions and attacks against Postal Service information resources per agreement with the Inspection Service.

d. Investigating the release or attempted release of malicious code onto Postal Service information resources.

e. Investigating use of Postal Service information resources to attack external networks.

f. Promoting efficiency in the operation of the Postal Service.

g. Funding CISO investigative efforts outside of those normally required.

h. The manager, Technical Crimes Unit (TCU), is responsible for the following:

(1) Functioning as an ongoing liaison with CyberSafe.

(2) Serving as a point of contact between CyberSafe and law enforcement agencies.

(3) Conducting criminal investigations of attacks upon Postal Service networks and computers.

2-2.18 Manager, Business Continuance Management

The manager, Business Continuance Management, is responsible for the following:

a. Protecting the health and safety of Postal Service employees.

b. Ensuring the continuity of business, expediting recovery from a loss of a single critical system or a major disruption to business functions.

c. Reviewing and assessing Business Continuity Management (BCM) program plans.

d. Defining, planning, developing, implementing, managing, assuring the testing and exercising, and monitoring for compliance of a sustainable BCM program for the Postal Service.

e. Ensuring appropriate Business Continuity Plans (BCPs) are developed, tested, and exercised for business functions and information technology services.

f. Ensuring appropriate DRP documents are developed and business information systems are tested for all critical and business functions and services.

g. Certifying all DRP test and BCP exercise.

h. Developing and implementing lines of communication to the IT organization about BCM matters.

i. Promoting BCM awareness and providing training for Postal Service personnel.

j. Ensuring compliance with BCM and information security policies.

k. Establishing BCM policy and strategy.

2-2.19 Manager, Telecommunications Services

The manager, Telecommunications Services (TS), is responsible for the following:

a. Implementing and maintaining operational information security throughout the network infrastructure including timely security patch management. Critical security patches for PCI-related information resources must be installed within 30 days of release.

b. Recommending and deploying network hardware and software based on the Postal Service security architecture.

c. Operational monitoring and tracking of all physical connections between any component of the Postal Service telecommunications infrastructure and any associated information resource not under Postal Service control.

d. Implementing security controls and processes to safeguard the availability and integrity of the Postal Service intranet including physical access to network infrastructure and the confidentiality of sensitive-enhanced and sensitive information.

e. Implementing the network perimeter firewalls, demilitarized zones, secure enclaves, and proxy servers.

f. Designating TS representative(s) to the NCRB.

g. Ensuring secure and appropriate connectivity to the Postal Service intranet.

h. Ensuring network services and protocols used by Postal Service information resources provide the appropriate level of security for the Postal Service intranet and the information transmitted.

i. Implementing secure methods of remote access and appropriate remote access controls.

j. Implementing two-factor authentication and the associated infrastructure for network management.

k. Implementing only Postal Service-approved encryption technology.

l. Implementing appropriate network security administration and managing accounts appropriately.

m. Maintaining the integrity of data and network information resources.

n. Supporting the implementation of approved security incident detection and prevention technologies (e.g., virus scanning, intrusion detection systems, and intrusion prevention systems) throughout the perimeter.

o. Maintaining an accurate inventory of Postal Service network information resources.

p. Monitoring network security alerts and logs and providing network security audit logs to the CISO ISS.

q. Ensuring that recovery plans and sufficient capacity are in place for the recovery of the telecommunications infrastructure for the IT-supported Postal Service sites.

r. Identifying and training key technical personnel to provide support in BCM for information resources housed in IT-supported Postal Service sites.

s. Monitoring network traffic for anomalies, conducting perimeter scanning for viruses, malicious code, and usage of nonstandard network protocols, and immediately reporting suspected information security incidents to CyberSafe.

t. Protecting information resources at risk during security incidents (if feasible) and providing support for CyberSafe incident containment and response.

u. Approving all wireless technology before any implementation activities are initiated.

v. Implementing and managing wireless local area network connectivity.

w. Detecting unauthorized access points.

x. Resolving identified vulnerabilities.

2-2.20 Managers Responsible for Computing Operations

The managers responsible for computing operations are responsible for the following:

a. Implementing information security policies, procedures, and standards and ensuring compliance.

b. Coordinating and implementing standard platform configurations based on the Postal Service security architecture.

c. Creating and maintaining a timely patch management process and deploying patches to resources under their control. Critical security patches for PCI-related information resources must be installed within 30 days of release.

d. Maintaining an accurate inventory of Postal Service information resources, tracking and reacting to security vulnerability alerts, coordinating hardware and software upgrades, and maintaining appropriate records.

e. Deploying and maintaining anti-virus software and recognition patterns to scan for malicious code and usage of nonstandard network protocols.

f. Supporting the C&A process for internally managed information resources.

g. Ensuring that remote access is appropriately managed.

h. Implementing appropriate security administration and ensuring that accounts are managed appropriately.

i. Maintaining the integrity of data and information resources and ensuring the appropriate level of information resource availability.

j. Ensuring the installation of the authorized internal warning banner (see Exhibit 14-3.3).

k. Disseminating security awareness and warning advisories to local users.

l. Reporting suspected information security incidents to CyberSafe immediately, protecting information resources at risk during security incidents, implementing containment, and assisting in restoring information resources following an attack.

m. Resolving identified vulnerabilities.

2-2.21 Manager, Corporate Information Security Office Information Systems Security

The manager, CISO ISS is responsible for the following:

a. Determining the requirements and standards for secure enclaves.

b. Assessing information resources to determine the need for placement in a secure enclave.

c. Provide oversight for standard configurations and hardening standards in collaboration with MPE/MHE System owners.

d. Approving two-factor authentication (e.g., digital certificates, digital signatures, biometrics, smart cards, and tokens) and the associated infrastructure for network management.

e. Approving and managing intrusion detection systems and intrusion prevention systems.

f. Approving, managing, and ensuring appropriate perimeter penetration testing and network vulnerability scans and testing.

g. Providing support to the OIG during the conduct of investigative activities concerning information security, the computing infrastructures, and network intrusion as requested.

h. Approving the use of networking monitoring tools, except those used by the OIG.

i. Providing support to the chief postal inspector during his or her conduct of site security reviews as requested.

j. Conducting monitoring and surveillance activities.

k. Collecting, correlating, and reviewing all Postal Service security audit log files and security alerts.

l. Reviewing information security policy and processes for MPE/MHE.

m. Developing and maintaining an information security architecture and coordinating a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.

n. Removing network connectivity from any computi ng device that does not meet the defined operating system and anti-virus software and recognition pattern thresholds.

o. Managing the NCRB to control connectivity to the Postal Service computing infrastructure.

p. Designating the chairperson of the NCRB and additional ISS representative(s) to the NCRB, as required.

q. Designating an information security policy and process program manager who is responsible for establishing, documenting, and disseminating information security policies, standards, and processes.

The manager, NCRB is responsible for the following:

a. Ensuring connectivity requests are submitted in the established format and sufficient in detail to be evaluated properly.

b. Contacting the submitter or technical contact for any additional or missing information.

c. Forwarding the approved connectivity request to the implementation organizations.

d. Providing technical guidance throughout the network connectivity process.

e. Analyzing business cases and supporting documents for connectivity requests.

f. Evaluating connectivity requests and approving or rejecting them based on existing policy and industry leading best practices.

g. Evaluating connectivity requests for Postal Service information resource to secure enclave needs.

h. Assisting the submitter in identifying alternative solutions for rejected requests that are acceptable to the submitter and comply with the Postal Service standards.

i. Reviewing new information resource, infrastructure, and network connections and their effects on overall Postal Service operations and information security.

j. Ensuring all changes made for an emergency request are annotated and submitted via the NCRB process as soon as work is complete.

k. Enforcing standard connectivity and documentation criteria to expedite approval of connectivity requests.

l. Determining criteria for standard connectivity that will allow for preapproved requests.

m. Ensuring compliance with Postal Service information system security policies and procedures, resources, and communications standards.

n. Identifying and reporting unauthorized or non-compliant connections in the Postal Service network to responsible parties.

o. Reviewing and monitoring business partner connectivity to ensure appropriate responses in event of a breach

p. Taking ownership of the NCRB process through stages leading up to Telecom Implementation

q. Performing evaluation and endorsement of Google chrome extensions.

r. Conducting regular training of teams new or unfamiliar with current NCRB policy and procedure.

The manager, CyberSafe is responsible for the following:

a. Providing immediate and effective response not to be restricted to including removal of malware infected device, but also implementing a recommended solution to the affected system owner to repair and restore functionality.

b. Working with an organization to contain, eradicate, document, and recover following a computer security incident. Coordinating with the stakeholders for incidents involving mail processing equipment.

c. Engaging other Postal Service organizations including, but not limited to, the OIG and Inspection Service.

d. Escalating information security issues to executive management as required.

e. Conducting a post-incident analysis, where appropriate, and recommending preventive actions.

f. Maintaining a repository for documenting, analyzing, and tracking Postal Service security incidents until they are closed.

g. Interfacing with other governmental agencies and private-sector computer incident response centers.

h. Participating in and providing lesson-learned information from information security incidents into ongoing information security awareness and training programs.

i. Developing and documenting processes for incident reporting and management.

j. Providing support to the OIG and the Inspection Service, as requested.

k. Managing CyberSafe to help the Postal Service contain, eradicate, document, and recover following a computer security incident and return to a normal operating state.

2-2.22 Managers, Help Desks

The managers, Help Desks, are responsible for the following:

a. Creating the entry for the problem tracking management system for security incidents reported to the Help Desks.

b. Providing technical assistance for responding to suspected virus incidents reported to the Help Desks.

c. Escalating unresolved suspected virus events to CyberSafe.

2-2.23 Contracting Officers and Contracting Officer Representatives

Contracting officers and contracting officer representatives are responsible for the following:

a. Ensuring that information technology suppliers, contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.

b. Thoroughly vetting service providers for PCI services prior to engagement that includes a risk analysis and documentation to reflect due diligence to the PCI assessor.

c. Updating the PCI Program Management Office (PMO) with status information on service providers for the PCI environment.

d. Verifying that information technology suppliers, vendors, and business partners responsible for storing, processing, or transmitting Postal Service payment card information complete an annual Letter of Attestation providing an acknowledgement of their responsibility for the security of payment card data, under the current PCI DSS.

e. Monitoring service provider PCI compliance at least annually.

f. Verifying that all contracts and business agreements requiring access to Postal Service information resources identify sensitive

positions, specify the clearance levels required for the work, and address appropriate security requirements.

g. Verifying that contracts and business agreements allow monitoring and auditing of any information resource project.

h. Verifying that the security provisions of the contract and business agreements are met.

i. Confirming the employment status and clearance of all contractors who request access to information resources.

j. Verifying all account references, building access, and other privileges are removed for contractor personnel when they are transferred or terminated.

k. Notifying CyberSafe of any security breaches reported to them by the service providers.

l. Directing the supplier to remedy code that is identified by the Executive Sponsor, IT Program Manager and CISO ISSO and taking such contractual action as necessary to enforce contract requirements.

m. In the case the CO/COR oversees a SOX relevant service provider, including PC Postage and/or meter vendors, the CO/COR is responsible for the following:

n.Receiving a System Organization Controls 1 (SOC1) report type II or equivalent report (e.g. FedRAMP, SOC2) if applicable, covering the relevant services provided to the US Postal Service.

o. Communicating with compliance and finance groups, on the cadence as requested by each team to discuss exceptions, issues and reporting

p.Complying with applicable regulations on the authorization to manufacture and distribute postage evidencing systems. (See 39 CFR Part 501).

q. In the case a third party is a new Postage Evidencing System (PES) provider to the US Postal Service, the party must adhere to the application guidelines proposed in the USPS Postage Evidencing System (PES) provider Applicant Onboarding Guide"

2-2.24 General Counsel

The general counsel is responsible for the following:

a. Ensuring that information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.

b. Ensuring that contracts and agreements allow monitoring and auditing of Postal Service information resource projects.

2-2.25 Business Partners

Business partners may request connectivity to Postal Service network facilities for legitimate business needs. Business partners requesting or using connectivity to Postal Service network facilities are responsible for the following:

a. Initiating a request for connectivity to the Postal Service executive who sponsors the request.

b. Complying with Postal Service network connectivity request (see Handbook AS-805-D, *Information Security Network Connectivity Process)* requirements and process.

c. Abiding by Postal Service information security policies regardless of where the systems are located or who operates them. This also includes strategic alliances.

d. Protecting information resources at risk during security incidents, if feaslble.

e. Maintain Chain of Custody for information assets exposed during security incidents, to track the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. To ensure the integrity of the evidence for post-incident review or law enforcement involvement.

f. Reporting information security incidents immediately to CyberSafe, the executive sponsor, and the information systems security officer (ISSO) assigned to their project.

g. Taking action, as directed by CyberSafe, to eradicate the incident, recover from it, and document actions regarding the security incident.

h. Allowing site security reviews by the Postal Inspection Service and CISO.

i. Allowing audits by the OIG.

j. Remediating deficiencies in their security posture as identified by the CISO Risk team during the Third-Party Cybersecurity Risk Assessments of contract requirements.

2-2.26 Accreditor

The manager, CISO, functions as the accreditor and is responsible for the following:

a. Reviewing the risk mitigation plan and supporting C&A documentation package together with business requirements and relevant Postal Service issues.

b. Escalating security concerns or preparing and signing an accreditation letter that makes one of the following recommendations: accepting the information resource with its existing information security controls, requiring additional security

controls with a timeline to implement, or deferring deployment until information security requirements can be met.

c. Forwarding the accreditation letter and C&A documentation package to the Business Relationship Management manager and executive sponsor.

2-2.27 Certifier

The manager, Security Certification and Accreditation Process, who is appointed by the manager, CISO, functions as the certifier and is responsible for the following:

a. Managing and providing guidance to the ISSOs.

b. Reviewing the C&A evaluation report and the supporting C&A documentation package.

c. Escalating security concerns or preparing and signing a certification letter.

d. Forwarding the certification letter and C&A documentation package to the accreditor.

e. Maintaining an inventory of all information resources that have completed the C&A process.

2-2.28 Security Control Officers

SCOs ensure the general security of the facilities to which they are appointed, including the safety of on-duty personnel and the security of mail, Postal Service funds, property, and records entrusted to them [see the *Administrative Support Manual* (ASM) 271.3, Security Control Officers]. SCOs are responsible for the following:

a. Establishing and maintaining overall physical and environmental security at the facility, with technical guidance from the Inspection Service.

b. Establishing controlled areas within the facility, where required, to protect information resources designated as sensitive-enhanced, sensitive, or critical.

c. Establishing and maintaining access control lists of people who are authorized access to specific controlled areas within the facility.

d. Ensuring positive identification and control of all personnel and visitors in the facility.

e. Ensuring the protection of servers, workstations, portable devices, and information located at the facility.

f. Consulting on the facility COOP plans.

g. Conducting annual facility security reviews using the site security survey provided by the Inspection Service.

h. Reporting suspected information security incidents to CyberSafe and providing support for incident containment and response, as requested.

i. Responding to physical security incidents and reporting physical security incidents to the Inspection Service.

j. Interfacing with CyberSafe, Inspection Service, CISO, or OIG, as required.

2-2.29 Information Systems Security Representatives

ISSRs are appointed in writing by the executive sponsors or the Business Relationship Management portfolio manager and are members of the information resource development or integration teams. The role of the ISSR can be performed in conjunction with other assigned duties. If an ISSR is not assigned, the project manager assumes the role. ISSRs are responsible for the following:

a. Providing support to the executive sponsor and Business Relationship Management portfolio manager, as required.

b. Promoting information security awareness on the project team.

c. Ensuring security controls and processes are implemented.

d. Notifying the executive sponsor, Business Relationship Management portfolio manager, and ISSO of any additional security risks or concerns that emerge during development or acquisition of the information resource.

e. Developing or reviewing security-related documents required by the C&A process as assigned by the executive sponsor or Business Relationship Management portfolio manager.

f. Working with the ISSO to complete the eC&A artifacts in the eC&A system and sending other required artifacts (e.g., TAD, operational training, etc.) or their location (i.e., URL) to the ISSO.

2-2.30 Information Systems Security Officers

ISSOs are responsible for the following:

a. Chairing the C&A team.

b. Ensuring that a BIA is completed for each information resource.

c. Ensuring that the responsible project manager records the sensitivity and criticality designations in EIR.

d. Advising and consulting with executive sponsors, Business Relationship Management portfolio managers, and ISSRs during the BIA process so they know the background for (1) baseline security requirements that apply to all information resources and (2) the security requirements necessary to protect an information resource based on the resource's sensitivity and criticality designation.

e. Recommending security requirements to executive sponsors and Business Relationship Management portfolio managers during the BIA process, based on generally accepted industry practices and the risks associated with the information resource.

f. Providing guidance on how information resources are vulnerable to threats, what controls and countermeasures are appropriate, and the C&A process.

g. Conducting site security reviews or helping the Inspection Service conduct them.

h. Reviewing the C&A documentation package.

i. Preparing and signing the C&A evaluation report and forwarding the evaluation report and C&A documentation to the certifier.

j. Coordinate with the IT SOX program on matters pertaining to the C&A documentation (i.e., Dataflow Mappings, Risk Acceptance Letters, Disaster Recovery Plans) for SOX in-scope applications.

2-2.31 Penetration Testers

Penetration Testing are responsible for performing testing activities at the direction of the CISO and Cybersecurity Risk Management. Additionally, the penetration testers shall complete the following:

a. Perform assessments using a variety of penetration testing tools on applications, infrastructure, and other information resources
b. Liaise on behalf of the CISO Risk Management to work with Business Project Leaders and System owners to gather information in support of penetration testing activities
c. Review findings discovered by penetration testing
d. Assist in planning and support of Red Team activities at the discretion of the CISO Risk Management
e. Ensure that validation related activities are performed in support of Vulnerability Remediation Management Team requirements
f. Informs the CISO Risk Management of any issues impeding progress towards successful penetration testing engagements
g. Compile penetration testing reports for review by CISO Risk Management
h. Provide technical assistance and expertise to CISO pertaining to specific vulnerabilities and findings within the enterprise.

2-2.32 System and Network Administrators

System and network administrators are technical personnel who serve as computer systems, network, server, and firewall administrators, whether the system management function is centralized, distributed, subcontracted, or outsourced. System and network administrators are responsible for the following:

a. Implementing information security policies and procedures for all information resources under their control, and also for monitoring the implementation for proper functioning of security mechanisms.

b. Implementing appropriate platform security based on the platform specific hardening standards for the information resources under their control.

c. Complying with standard configuration settings, services, protocols, and change control procedures.

d. Applying approved patches and modifications in accordance with policies and procedures established by the Postal Service. Ensuring that security patches and bug fixes are kept current for resources under their control.

e. Implementing appropriate security administration and ensuring that log-on IDs are unique.

f. Setting up and managing accounts for information resources under their control in accordance with policies and procedures established by the Postal Service.

g. Disabling accounts of personnel whose employment has been terminated, who have been transferred, or whose accounts have been inactive for an extended period of time.

h. Making the final disposition (e.g., deletion) of the accounts and the information stored under those accounts.

i. Managing sessions and authentication and implementing account time-outs.

j. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.

k. Testing information resources to ensure security mechanisms are functioning properly.

l. Tracking hardware and software vulnerabilities.

m. Maintaining an accurate inventory of Postal Service information resources under their control.

n. Ensuring that audit and operational logs, as appropriate for the specific platform, are implemented, monitored, protected from unauthorized disclosure or modification, and are retained for the time period specified by Postal Service security policy.

o. Reviewing audit and operational logs and maintaining records of the reviews.

p. Identifying anomalies and possible internal and external attacks on Postal Service information resources.

q. Reporting information security incidents and anomalies to their manager and CyberSafe immediately upon detecting or receiving notice of a security incident.

r. Protecting information resources at risk during security incidents, assisting in the containment of security incidents as required, and taking action as directed by CyberSafe.

s. Participating in follow-up calls with CyberSafe and fixing issues identified following an incident.

t. Ensuring that virus protection software and signature files are updated and kept current for resources under their control.

u. Ensuring the availability of information resources by implementing backup and recovery procedures.

v. Ensuring the compliance with Postal Service information security policy and procedures.

w. Monitoring the implementation of network security mechanisms to ensure that they are functioning properly and are in compliance with established security policies.

x. Maintaining a record of all monitoring activities for information resources under their control.

y. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.

z. Resolving identified vulnerabilities.

2-2.33 Database Administrators

Database administrators (DBAs) are responsible for the following:

a. Implementing appropriate database security based on the platform specific hardening standards for the information resources under their control.

b. Implementing information security policies and procedures for all database platforms and monitoring the implementation of database security mechanisms to ensure that they are functioning properly and are in compliance with established policies.

c. Applying approved patches and modifications, in accordance with policies and procedures established by the Postal Service.

d. Maintaining an accurate inventory of Postal Service information resources under their control.

e. Implementing appropriate database security administration and ensuring that log-on IDs are unique.

f. Setting up and managing accounts for systems under their control in accordance with policies and procedures established by the Postal Service.

g. Disabling accounts of personnel that have been terminated, transferred, or have accounts that have been inactive for an extended period of time.

h. Making the final disposition (e.g., deletion) of the accounts and the information stored under those accounts.

i. Managing sessions and authentication and implementing account time-outs.

j. Preventing residual data from exposure to unauthorized users as information resources are released or reallocated.

k. Testing database software to ensure that security mechanisms are functioning properly.

l. Tracking database software vulnerabilities, and deploying database security patches.

m. Ensuring database logs are turned on, logging appropriate information, protected from unauthorized disclosure or modification, and retained for the time period specified.

n. Reviewing database audit logs and maintaining records of log reviews.

o. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.

p. Ensuring the availability of databases by implementing database backup and recovery procedures.

q. Identifying anomalies and possible attacks on Postal Service information resources.

r. Reporting information security incidents and anomalies to their manager and CyberSafe immediately upon detecting or receiving notice of a security incident.

s. Protecting information resources at risk during security incidents, assisting in the containment of security incidents as required, and taking action as directed by CyberSafe.

t. Resolving identified vulnerabilities.

2-2.34 All Personnel

All personnel, including employees, suppliers, consultants, contractors, business partners, customers who access non-publicly available Postal Service information resources (e.g., mainframes or the internal Postal Service network), and other authorized users of Postal Service information resources are responsible for the following:

a. Complying with applicable laws, regulations, and Postal Service information security policies, standards, and procedures.

b. Displaying proper identification while in any facility that provides access to Postal Service information resources.

c. Being aware of their physical surroundings, including weaknesses in physical security and the presence of any authorized or unauthorized visitor.

d. Protecting information resources, including workstations, portable devices, information, and media.

e. Always using their physical and technology electromechanical access control identification badge or device to gain entrance to a controlled area.

f. Ensuring no one tailgates into a controlled area on their badge.

g. Performing the security functions and duties associated with their job, including the safeguarding of their log-on IDs and passwords.

h. Changing their password immediately, if they suspect that the password has been compromised.

i. Prohibiting any use of their accounts, log-on IDs, passwords, personal information numbers (PINs), and tokens by another individual.

j. Taking immediate action to protect the information resources at risk upon discovering a security deficiency or violation.

k. Only using licensed and approved hardware and software.

l. Protecting intellectual property.

m. Complying with Postal Service remote access information security policies, including those for virtual private networks, modem access, dial-in access, secure telecommuting, and remote management and maintenance.

n. Complying with acceptable use policies.

o. Maintaining an accurate inventory of information resources for which they are responsible.

p. Protecting information resources against viruses and malicious code.

q. Calling the appropriate Help Desk for technical assistance in response to suspected virus incidents.

r. Immediately reporting to CyberSafe via telephone or email and, as appropriate, to their immediate supervisor, manager, or system administrator, any suspected security incidents, including security violations or suspicious actions, suspicion or occurrence of any fraudulent activity; unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information; and potentially dangerous activities or conditions.

s. Taking action, as directed by CyberSafe, to protect against information security incidents, to contain and eradicate them when they occur, and to recover from them.

t. Documenting all conversations and actions regarding the security incident and completing PS Form 1360, *Information Security Incident Report,* or an acceptable facsimile.

u. If an individual removes a portable electronic device from a Postal Service facility, he or she must do the following:

(1) If the device contains sensitive-enhanced or sensitive information, request approval in writing from his or her functional area vice president (data steward), CPO, and the VP IT Operations or their designees.

(2) Protect the device and the data it contains.

(3) Keep the device within sight, secured with a cable lock, or locked in a cabinet or closet.

(4) Do not check the device in baggage on an airplane, train, or any other public transportation.

(5) If an individual must leave the device in his or her vehicle, keep the device out of sight in a locked trunk. Never leave the device in a vehicle overnight.

(6) Use Postal Service-approved encrypted flash drive or encrypt sensitive-enhanced and sensitive data on the hard drive or other removable media using WinZip or Encryption File System (EFS).

v. Reporting any missing or stolen device or media immediately to his or her manager, CyberSafe via e-mail to *CyberSafe@usps.gov,* and to the local Inspection Service office. If the device has been stolen somewhere other than Postal Service premises, report the theft to the local police as well.

w. Complete all security training required by the Postal Service for their specific role.

3 Information Designation and Control

3-1 Policy

Postal Service information resources must be protected from time of collection to retirement, disposal, and destruction commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Postal Service's ability to conduct its mission.

All personnel must implement the protection requirements for information resources associated with information designation, categorization, and protection (including labeling, handling, controlling access and retention, protecting in transit and in storage, disposal, and destruction).

The following roles are vital to the protection of Postal Service Information:

a. The data owner is the executive with statutory and operational authority or specified information and responsibility for overseeing its generation, collection, processing, dissemination, disposal, and for the business results from using the information. The owner is responsible for ensuring that appropriate steps are taken to protect the information and for the implementation of policies, guidelines, and memorandums of understanding that define the appropriate use of the information.

b. The data steward is the manager with responsibility for providing business users with high-quality data that is easily accessible in a consistent manner. Data stewardship focuses on tactical coordination and implementation. Data stewards are responsible for carrying out data usage and security policies determined by the data owner or through enterprise data governance initiatives. Data stewards provide agreed-upon data definitions and formats and ensure that business users adhere to specified standards. They often collaborate with data architects; business intelligence developers; extraction, transformation, and load (ETL) designers; business data owners; and others to uphold data consistency and data quality metrics.

c. The data custodian is responsible for administrative and operational control over the information and for granting access to the information based on direction provided by the data steward.

Chapter 3 addresses the following:

a. Information designation and categorization.

b. Determination of the categorization of information resources.

c. Security requirements categories.

d. Protection of Postal Service information and media.

e. Protection of non-Postal Service information.

The Postal Service must develop data security policies using a set of data security standards, guidelines and requirements based on industry best practices that reflect levels of sensitivity further defined in this chapter according to privacy, access, retention, disposal, incident management, disaster recovery, and configuration management. Data or information designation, classification, and control is the process of sorting data or information into groups based on sensitivity and/or criticality.

In essence, a classification system contains all data at a particular level of criticality, or sensitivity. Classifications allow the organization to make rational decisions about the value of data of a certain type. The Postal Service will assign an appropriate degree of control for each type based on business value. The assignment creates layered groups of control at different levels of sensitivity and/or criticality.

The items in the group of highest priority are fully protected, while items of lesser value will still be given some protection appropriate to their relative status in the priority queue.

The term that is commonly used to describe the outcome of a classification process is "defense in depth." Classification levels are implemented hierarchically; each successive layer describes an increasingly rigorous degree of control, which is required to ensure integrity. Every level implements a well-defined set of rules that ensures that access is restricted only to those individuals who have been authorized. Establishing classification levels within an organization controls the resource allocation process efficiently for compliance. The classification definitions allow the Postal Service to make intelligent choices about how to protect three simple groupings of data rather than an uncounted number, or ad-hoc division of individual items. In conventional practice, these three groupings are labeled "unclassified" (any item of data that has not received a classification as defined by the USPIS as national security), "classified", and "classified under Executive Order 13526 or the Atomic Energy Act", as amended.

3-2 Information Designation and Categorization

Information at the Postal Service is designated and categorized based on the classification, sensitivity, and criticality of the information.

3-2.1 Potential Impact and Risk of Harm

All Postal Service personnel who have access to sensitive and sensitive enhanced information have a duty and responsibility to safeguard and protect the confidentiality and integrity of sensitive and sensitive-enhanced business and personal information against theft, unauthorized access, disclosure, along with manipulation or misuse of Postal Service information.

Such actions could result in substantial harm to the Postal Service brand, its business operations, financial operations and information systems, along with embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. Examples of harm include loss of control or misuse of information, damage to the trusted Postal Service brand, financial 3-2.4.1

loss, fiscal damage, exposure to possible law suits, and other negative impacts which adversely affect one or more individuals through fraud, manipulation or identity theft, or undermine the integrity of a system or program.

3-2.2 Designation Categories and Levels

Exhibit 3-2.2 defines classification, sensitivity, and criticality designation categories and levels.

Exhibit 3-2.2
Designation Categories and Levels

Designation Category	Description	Levels *(In decreasing order of necessity to protect the confidentiality, integrity, and availability of the information)*
Classification	Classification levels determine the need to protect the confidentiality and integrity of information.	Classified – Hardcopy or electronic information or material that has been designated as classified pursuant to executive order, statue, or regulation and requires protection against unauthorized disclosure for reasons of national security. Unclassified – Hardcopy or electronic information or materials that includes both sensitive but unclassified and non-sensitive which at a minimum must be safeguarded against tampering, destruction or loss.
Sensitivity	Sensitivity determines the need to protect the confidentiality and integrity of sensitive information.	Sensitive-Enhanced Unclassified Information (hereafter referred to as Sensitive-Enhanced) Sensitive Unclassified Information (hereafter referred to as Sensitive) Non-sensitive Unclassified Information (hereafter referred to as Non-sensitive)
Criticality	Criticality reflects the need for continuous availability of the information.	Critical (High) Critical (Moderate) Noncritical

3-2.3 Sensitivity and Criticality Category Independence

Sensitivity and criticality are independent designations. All Postal Service information must be evaluated to determine both sensitivity and criticality. Information with any sensitivity level may have any level of criticality level and vice versa.

3-2.4 Definitions of Classified, Sensitive, and Critical Information

3-2.4.1 Classified Information

Classified information is hardcopy or electronic information or material that has been designated as classified pursuant to executive order, statue, or regulation and requires protection against unauthorized disclosure for reasons of national security. National security reasons includes national defense, foreign relations of the United States, intelligence activities, atomic weapons and special nuclear material, crypto logic activities related to national security, command and control of military forces, integral components of weapon systems, or critical to direct fulfillment of military or 3-

2.4.2 intelligence missions. Classified designations include Confidential, Secret, and Top Secret. Categories of classified information include restricted data (RD), formerly restricted data (FRD), and national security information (NSI).

Note: Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

3-2.4.2 Sensitive-Enhanced Information

Sensitive-enhanced information is hardcopy or electronic information or material that is not designated as classified but that warrants or requires enhanced protection. Requirements to protect sensitive-enhanced information are derived from law, regulation, the law enforcement and judicial process, the payment card industry (PCI), and the Privacy Act. Types of sensitive-enhanced information include:

a. Law enforcement information and court-restricted information, including grand jury material, arrest records, and information about ongoing investigations.

b. PCI primary account number (PAN); i.e., full credit card number (16 characters).

c. Personally identifiable information (PII); i.e., information used to distinguish or trace an individual's identity such as name, Social Security number, driver license number, passport number, bank routing with account number, date with place of birth, mother's maiden name, biometric data, and any other information which is linked or linkable to an individual.

d. Information about individuals (e.g., employees, contractors, vendors, business partners, and customers) protected by law, including medical information and wire or money transfers.

e. Information related to the protection of Postal Service restricted financial information, trade secrets, proprietary information, and emergency preparedness.

f. Communications protected by legal privileges (e.g., attorney-client communications encompassing attorney opinions based on client supplied information) and documents constituting attorney work products (created in reasonable anticipation of litigation).

3-2.4.3 Sensitive Information

Sensitive information is hardcopy or electronic information or material that is not designated as classified or sensitive-enhanced but that warrants or requires protection. Requirements to protect sensitive information are derived from law, regulation, the Privacy Act, business needs, and the contracting process. Types of sensitive information include:

a. Private information about individuals (e.g., employees, contractors, vendors, business partners, and customers) including marital status, age, birth date, race, and buying habits.

b. Confidential business information that does not warrant sensitive-enhanced protection including trade secrets, proprietary information, financial information, contractor bid or proposal information, and source selection information.

c. Data susceptible to fraud including accounts payable, accounts receivable, payroll, and travel reimbursement.

d. Information illustrating or disclosing information resource protection vulnerabilities, or threats against persons, systems, operations, or facilities such as physical, technical or network/DMZ/enclave/ mainframe/server/workstation specifics including security settings, passwords, and audit logs.

3-2.4.4 Non-sensitive Information

Information that is not designated as classified, sensitive-enhanced, or sensitive information is by default designated as non-sensitive information. An example is publicly available information. Even though information is designated as non-sensitive information, it must still be protected (i.e., baseline requirements apply to all Postal Service information). Non-publicly available information must not be sent over the Internet unprotected (e.g., unencrypted).

3-2.4.5 Critical (High) Information

Information is designated as critical (high) information if its unavailability would have a catastrophic adverse impact on the following:

a. Customer or employee life, safety, or health.
b. Payment to suppliers or employees.
c. Revenue collection.
d. Movement of mail.
e. Communications.
f. Legal or regulatory.

3-2.4.6 Critical (Moderate) Information

Information is designated as critical (moderate) information if its unavailability would have a serious adverse impact on the following:

a. Customer or employee life, safety, or health.
b. Payment to suppliers or employees.
c. Revenue collection.
d. Movement of mail.
e. Communications.
f. Legal or regulatory.
g. Infrastructure services.

3-2.4.7 Noncritical Information

Information that is not designated as critical (high) or critical (moderate) is by default designated as noncritical.

3-3 Determination of the Categorization of Information Resources

3-3.1 Business Impact Assessment

Business Impact Assessment (BIA) is the process of identifying the consequences of current or proposed actions. The "impact" is the difference between what would happen with the action and what would happen without it. The Postal Service uses the following two types of impact assessments:

a. Internal.
b. External.

3-3.1.1 Internal Business Impact Assessment

The Internal Business Impact Assessment (BIA) is a process for determining the categorization of Postal Service information resources. A BIA must be completed for all information resources, whether the information resource is developed in house, outsourced or hosted in non-Postal Service facilities. The BIA must be updated periodically as required (every one or three years depending on its sensitivity designation), whenever a significant change is made to the information resource, or whenever the certification and accreditation (C&A) process is re-initiated.

The criteria for initiating a recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process,* 6-2.

Various stakeholders [e.g., management, operational personnel, and information systems security officers (ISSOs)] need to be involved in the BIA process. An information resource may process several information types. Each information type is subject to security categorization. The stakeholders must consider the consequences of unauthorized disclosure of sensitive-enhanced or sensitive information with respect to violations of federal policy and law. The impact of the violations will depend in part on the penalties associated with violation of the relevant statutes and policies. A privacy impact assessment (PIA) is included in the BIA.

The impact level for an information resource will normally be the highest impact level for the following security objectives associated with the information types:

a. Confidentiality — Preserving authorized restrictions on information access and disclosure.
b. Integrity — Guarding against improper information modification or destruction.
c. Availability — Ensuring timely and reliable access to information.

However in some cases, the security category for a system may be higher than any impact level for any information type processed by the system. Variations in sensitivity/criticality with respect to time may also need to be factored into the impact assessment process. Some information loses its sensitivity in time (e.g., a Postal Service rate increase becomes non-sensitive after it has been published). Some applications are particularly critical at

some point in time (e.g., the payroll application on the day for normal processing).

3-3.1.2 External Assessments

Security provisions are carried out by the Cloud Service Provider (CSP). Postal Service data is stored in a custom database schema designed by the provider. The Postal Service does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings. The CSP must ensure Postal Service data is protected from unauthorized access, use, disclosure, disruption, modification or destruction to ensure integrity, confidentiality, and availability. The CSP must comply with the current version of the Payment Card Industry (PCI) Data Security Standard (DSS) and the Information Supplement PCI/DSS Cloud Computing Guidelines. All cloud solutions must demonstrate the ability to meet the Postal Service security requirements.

The Postal Service requires external providers handling Postal data and/or information resources or operating systems to meet the same security standards and requirements as internal users. The Postal Service must ensure that privacy and security controls and safeguards are implemented with maximum operational functionality to meet baseline privacy and security requirements and employ risk mitigation strategies and assessments.

3-3.1.3 Cloud Computing Impact Assessment.

The Consolidated Cloud Computing Impact Assessment (CCIA) is part of the Cloud Computing Certification and Accreditation security evaluation and assessment process. It is used to gather initial information on a cloud solution operating on a FedRAMP certified infrastructure. Refer to Handbook AS-805H, *Cloud Computing,* which includes responsibilities and instructions for completing the questionnaire. In most cases, the Information Systems Security Officer (ISSO) along with the Information systems security representatives (ISSR) will complete the questionnaire section of this document.

The purpose of the Consolidated Cloud Computing Impact Assessment is to identify the appropriate privacy and security requirements to protect Postal Service information resources, organization, and personnel.

The Consolidated CCIA ensures that cloud systems processing or storing customer or personnel information, or technologies that can be used for monitoring purposes adhere to Postal Service privacy requirements. Privacy requirements are based on applicable privacy laws, such as the Privacy Act, as well as privacy policies that the Postal Service has adopted. Compliance with privacy requirements is addressed in Section 4 of the Questionnaire.

3-3.2 Aggregation

Some information may have little or no sensitivity in isolation but may have high sensitivity in aggregate. In some cases, aggregation of large quantities of a single information type can reveal patterns and/or plans, or facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous information types

can have similar effects. In general, the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of a bank account number with the identity of an individual and/or institution).

The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system categorization may need to be adjusted to a higher level than would be indicated by the impact associated with any individual information type.

3-3.3 System Functionality

Compromise of some information types may have low impact in the context of a system's primary function but may have much more significance when viewed in the context of the potential impact of compromising:

a. Other systems to which the system in question is connected, or

b. Other systems which are dependent on that system's information.

Access control information for a system that processes only low-impact information might initially be thought to have only low-impact attributes. However, if access to that system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered.

Similarly, some information may, in general, have low-sensitivity or criticality attributes. However, that information may be used by other systems to enable sensitive-enhanced, sensitive, or critical functions. Loss of data integrity, availability, temporal context, or other context can have severe consequences.

3-3.4 Critical National Infrastructure

Where the mission served by an information system, or the information that the system processes affects the security of the critical national infrastructure, the loss of confidentiality, integrity, or availability could result in a higher designation.

3-3.5 Approving Information Resource Classification and Categories of Information Processed

The determination of the sensitivity for each information resource and the categories of information processed must be approved by the chief privacy officer (CPO) or his or her designee through the BIA. The determination of the criticality for each information resource must be approved by the postmaster general and his senior executives. This process is facilitated by the manager of Business Continuance Management or his or her designee.

3-3.6 Recording Information Resource Classification and Categories of Information Processed

The sensitivity and criticality for each information resource and the categories of information processed must be documented in the Enterprise Information Repository (EIR) and in the information security plan.

3-4 Security Requirement Categories

The Postal Service uses several categories of security requirements to protect information resources (see Exhibit 3-4).

A security requirement is a type or level of protection that must be implemented to secure an information resource. A control consists of safeguards designed to respond to a security requirement. A control may satisfy more than one requirement, or several controls may be needed to satisfy a security requirement depending on the sensitivity and criticality of the information resource and its operating environment. If a requirement cannot be addressed, compensating controls can be implemented to mitigate the risk.

Exhibit 3-4
Security Requirement Categories

Security Requirement Category	Control(s)
Baseline	All information resources must implement controls sufficient to satisfy the baseline security requirements. Baseline security requirements have been established to protect the Postal Service computing environment and infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction.
Sensitive-Enhanced, Sensitive, PCI, Law Enforcement, Critical (High), and Critical (Moderate)	Additional security is needed to adequately protect sensitive-enhanced, sensitive, and critical information resources. These requirements are based on the following: ■ Sensitivity and criticality of the information resource. ■ Federal legislation [e.g., the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act. ■ Federal regulations (e.g., requirements for cryptographic modules). ■ Federal directives (e.g., personal identity verification and critical infrastructure). ■ Industry requirements (e.g., all developers and service providers of PCI in-scope applications must comply with the current PCI Data Security Standard).
Conditional	Requirements requested by the executive VP and CIO; VP IT Solutions; Director IT Operations; manager, CISO; or the functional VP or requirements based on specific criteria such as the development and operating environment.
Recommended	ISSOs may recommend additional security requirements during the BIA process to better protect the information resource against threats and vulnerabilities. Recommended security requirements are based on generally accepted industry practices. The executive sponsor assumes the risks associated with not implementing the recommended security requirements.

3-5 Protection of Postal Service Information and Media

All Postal Service information must be properly handled and controlled. While the focus of information security is on protecting sensitive-enhanced and sensitive information which is driven by government regulation and industry standards, the Postal Service must also protect non-publicly available

information. Non-publicly available information must be protected by the same controls as sensitive and sensitive-enhanced information, e.g., encryption. If there are questions concerning the appropriate security controls to implement, consult with CISO.

The level of protection must be based on the information's sensitivity and criticality, e.g., full and partial social security numbers must only be used for tax purposes and must not be used for identification purposes and must not be printed on reports.

Labeling, retention, storage, encryption, release, and destruction of information must comply with the Postal Service policies specified in this section and in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management.*

3-5.1 Labeling of Information, Media, and Devices

3-5.1.1 Electronic Media and Hardcopy Output

The Postal Service processes, stores, and transmits many types of sensitive information. Appropriately labeling the media helps ensure that all recipients of the material are aware that the information requires protection.

Note: If information with different levels of sensitivity is combined, the total package must be protected at the sensitivity level of the information that has the greatest sensitivity.

The following definitions apply within this section:

a. Hardcopy Material – Printed material, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

b. Label – A RESTRICTED label may be internal or external as follows:

(1) Internal Label – A RESTRICTED marking within the confines of the medium.

(2) External Label – A RESTRICTED marking on the outside of the medium, or a cover.

c. Storage Media – Includes but is not limited to magnetic storage media such as hard disk drives and diskettes; optical storage media such as CDs and DVDs; solid-state storage media, including USB drives; and hardcopy materials, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

3-5.1.2 Applications Processing

On applications processing sensitive-enhanced or sensitive information, the following statement must be prominently displayed on the login/password screen or the welcome screen: "Information within this application is designated sensitive-enhanced (or sensitive) and should be properly protected from unauthorized access or disclosure." Additionally, the "Print Screen" function can also result in hardcopy that must be legibly and durably labeled as "RESTRICTED INFORMATION."

3-5.1.3 Devices

All in-scope PCI devices must be labeled with owner, contact information, and purpose.

3-5.2 Controlling Access to Information

Access to information in hardcopy and digital form must be restricted to authorized personnel as follows:

a. To prevent unauthorized access to hardcopy and electronic media, one of the following controls must be employed:

(1) A locked desk or file cabinet.

(2) A room with a key, combination, or electronic lock.

(3) An approved media storage area or an area behind a guard.

b. To prevent unauthorized access to electronic files and databases, access controls must be employed. Access attempts granted and refused are subject to audit.

c. Sensitive-enhanced and sensitive information must be protected from unauthorized access and disclosure. Access must be restricted to authorized personnel with a need to know. The functional system coordinator (FSC), as an agent of the executive sponsor (data steward), controls access based on role and level of access requested.

d. Metadata (i.e., data describing the structure, content, and context of electronic information) must also be protected from unauthorized access and disclosure.

e. Critical information must be protected from unauthorized access and destruction.

f. The PCI primary account number (PAN) must be masked when displayed and/or printed (the first six or the last four digits are the maximum digits that may be displayed or printed), such that only personnel with a legitimate business need for the information to perform their job (e.g., to process or manage transactions or chargebacks) can see the full PAN.

g. PANs must be de-identified or removed from tables, files, removable media, and audit logs.

h. All personnel with authorization to handle and/or view cardholder data must follow the PCI Data Security Standard (DSS) requirements to protect this type of sensitive-enhanced data.

3-5.3 Retention and Storage of Information

The retention and storage of information must be controlled as follows:

a. All Postal Service information must be retained in accordance with legal retention requirements established by law (e.g., legal holds), and also with operational retention requirements established by the business owner with concurrence by the Postal Service Privacy and Records Office, Legal, and the Inspection Service (see Handbook AS-353).

b. When the retention period or legal hold has expired, sensitive-enhanced, sensitive, and critical information must be properly destroyed as described in *Disposal and Destruction of Information and Media*. The process of removing expired information can be automated or manual.

c. Sensitive-enhanced, sensitive, and critical information should be stored in a controlled area or a locked cabinet in accordance with established Postal Service policies and procedures.

d. PII must not be stored or accessed on devices that are located outside of the United States.

e. Sensitive-enhanced information must not be processed or stored in a public cloud.

f. PCI and law enforcement information must be stored in an enclave.

g. Under no circumstances should non-publicly available information be stored on a public Web site.

h. Non-publicly available Postal Service information must be isolated and stored separately from non-Postal Service information (e.g., business partner and vendor information) unless required by law or regulation. Non-publicly available Postal Service information and non-Postal Service information must be stored separately at Postal Service facilities, non-Postal Service facilities, or at backup sites unless required by law or regulation.

i. Payment cardholder information must not be copied or stored on local hard drives or removable electronic media as the result of accessing such data via remote access technologies.

j. Payment cardholder electronic media must be inventoried and the inventory reconciled semiannually.

k. Cardholder data storage must be kept to a minimum and retention time must be limited.

l. The following PCI authentication data must not be stored (e.g., log files, history files, trace files, database contents, etc.) after completing the payment transaction under any circumstance:

   (1) The full contents of any track from the magnetic stripe on the back of the card or contained in a chip on the card.

   (2) The three-digit or four-digit card-validation code printed on the front of the card or the signature panel on the back of the card.

   (3) PINs or the encrypted PIN blocks.

m. Temporary storage of PCI authentication data must be deleted in a manner that makes the data unrecoverable.

n. PANs must be rendered unreadable anywhere they are stored by one way hash, truncation, indexed tokens, or strong cryptography.

o. Retention of payment card data is defined in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*. A quarterly automatic or manual process must be implemented for identifying and securely deleting cardholder data that exceeds the defined retention requirement.

p. Program-level and project-level TSLC artifacts and compliance records must be kept as long as the program/project is active and must be purged 27 months after the program/project is retired.

3-5.4 Encryption of Information

Examples of conditions under which Postal Service information must be encrypted include, but are not limited to, the following:

a. Sensitive-enhanced and sensitive information in transit across networks.

b. Sensitive-enhanced and sensitive data in transit between [1] an application or batch server and a database server and [2] between workstations and a database server.

c. Sensitive-enhanced and sensitive information at rest including information stored or archived on removable devices or media including disks, diskettes, CDs, and USB storage devices.

d. Sensitive-enhanced and sensitive information that is stored off Postal Service premises.

e. PCI information (encrypted throughout the life cycle).

f. Non-publicly available electronic information in transit or stored off Postal Service premises.

g. For portable Public Key Infrastructure (PKI) backup media, see 9-7.1 for encryption compliance methods.

3-5.5 Mandatory Requirements and Procedures for Authorized Removal of Postal Service Non-Publicly Available Information from Postal Service or Business Partner Premises

3-5.5.1 Definition of Non-Publicly Available Information

Non-publicly available information includes

a. Sensitive-enhanced information (see 3-2.4.2).

b. Sensitive information (see 3-2.4.3).

c. Non-sensitive information that the Postal Service does not want to disclose at this time.

3-5.5.2 Definition of Removal from Postal Service or Business Partner Premises

Removal from Postal Service or business partner premises includes:

a. Removal by remote access, with (or without) downloading or forwarding.

b. Removal by directed transmission through third-party services.

c. Removal from premises of digital copies stored on portable computers or any type of media.

d. Removal from premises in hard-copy format.

e. Printing off premises.

f. Sending a facsimile off premises.

g. Contractor shredding or destruction off premises.

h. Information directly collected on behalf of the Postal Service by a Business Partner or third-party service provider, e.g., an application that is externally hosted with all data collected by the Business Partner.

i. Information sent to a Business Partner as part of a Service-Based Contract.

3-5.5.3 Mandatory Requirements and Procedures for Authorized Removal Of Electronic and Hard-copy Information

The removal authorization must be approved in eAccess/ARIS and a list of all personnel with removal authorization must be available on request.

Before removal, the following approvals are required:

(1) Functional VP or designee (data steward).

(2) CPO or designee.

(3) CIO or CIO's designee (data custodian).

a. All physical functions (e.g., pickup, acceptance, reception, transfer, or delivery) related to removal of non-publicly available information must be conducted by authorized personnel whose identity is verified by a check of the Postal Service badge.

b. Two-factor authentication is required for electronic access or removal.

c. All non-publicly available electronic information that is accessed, processed, or stored at non-Postal Service sites must be encrypted and processed on either (1) Postal Service-owned hardware and software (2) on business-partner-owned hardware and software that meets all of the following requirements:

(1) Offsite Hosting Letter approved by:

(a) Functional VP or designee.

(b) Manager, CISO or designee.

(c) CIO or designee.

(2) Written stipulation that it meets Postal Service server hardening and malicious code protection standards.

(3) Written consent to unannounced audits.

e. All ACE-supported infrastructure components in use must be connected at least weekly over a secure link to the Postal Service intranet to receive appropriate security patches and virus recognition patterns.

Non-ACE-supported components must be appropriately patched and have the latest virus recognitions patterns installed.

f. All non-publicly available electronic information must be encrypted as follows:

(1) All types of storage off Postal Service premises including mobile devices such as laptops and portable media.

(2) All transmissions.

g. PCI cardholder information must not be stored off Postal Service premises on any device or media, including: hard drives, USB thumb drives, disks, PDAs, cell phones, or laptops.

h. All Postal Service (and/or business-partner-owned) electronic devices and electronic media (including backups) containing non-publicly available information and all hard copies must be effectively secured against theft and/or unauthorized access (e.g., controlled areas, safes, locked cabinets).

i. All removals of non-publicly available information must be concurrently documented to ensure accountability in the life cycle management of that information. All such data and all copies must be inventoried annually and formally tracked (e.g., logbook, tape management system) from creation to destruction. This inventory and tracking log must be updated with each transfer/removal and be available for audit.

3-5.6 Release of Information

The release of information must be accomplished in accordance with Postal Service policies and procedures (see Handbook AS-353).

Sensitive-enhanced and sensitive information must be protected from unauthorized disclosure, whether formally or informally through conversations, e-mail, voice, printing, facsimile, shredding, destruction, and observed workstation screens or whiteboards.

3-5.6.1 Releasing Information on Factory-Fresh or Degaussed Media

Before releasing information on electronic media outside the Postal Service, the information must be copied onto factory-fresh media (never used) or onto media that was appropriately degaussed to prevent inadvertent release of sensitive-enhanced and sensitive information.

3-5.6.2 Precautions Prior to Maintenance

To prevent inadvertent disclosure of sensitive-enhanced and sensitive information, all hardware and electronic media being released for maintenance outside of Postal Service facilities must, prior to release, undergo data eradication according to approved Postal Service procedures. If electronic media containing sensitive-enhanced and sensitive information is released to a contractor or vendor for maintenance, the Postal Service must have in place a legally binding contract regarding the secure handling and storage of the data or media.

3-5.7 Handling Biohazard Contaminated Information Resources

3-5.7.1 Sensitive-Enhanced and Sensitive Information

Any personnel handling biohazard contaminated Postal Service information resources must follow the standards set forth by the Inspection Service for handling contaminated devices. If the contaminated information resource contains sensitive-enhanced and sensitive information, the Inspection Service must be notified regarding the type of device, the classification of data it contains (i.e., sensitive-enhanced or sensitive), and the Postal Service

manager responsible for the device. Disposition of the contaminated information resource must be recorded, including who took possession of the device and the disposition expected for the resource.

3-5.7.2 Data Eradication on Contaminated Information Resources

Any Postal Service hardware or electronic media being released outside of Postal Service facilities must, prior to release, undergo data eradication, if possible, according to approved Postal Service procedures. Eradication procedures may include the ability to eradicate data through remote management of the information resource. If data eradication is not possible, the Inspection Service must be advised and notification must be made to all persons involved in the chain of possession of their responsibility for nondisclosure of the information contained in the device. It is strongly recommended that a memorandum of nondisclosure be signed by all personnel involved in the chain of possession of the contaminated information resource.

3-5.7.3 Reporting of Contaminated Information Resources

The Postal Service manager responsible for the contaminated device must complete PS Form 1360, *Information Systems Security Incident Report,* to ensure appropriate security management notification of the status and disposition of the information resource.

3-5.8 Disposal and Destruction of Information and Media

3-5.8.1 Electronic Hardware and Media

To prevent inadvertent disclosure of sensitive-enhanced and sensitive information, all electronic hardware and media must, prior to being disposed of, undergo data eradication according to approved Postal Service procedures. Unacceptable practices of erasure include a high-level file erase or high-level formatting that only removes the address location of the file. Acceptable methods of complete erasure include the following:

a. Zero-bit formatting
b. Degaussing
c. Physical destruction
d. Crypto Erasure or Crypto Shredding

The results from zero-bit formatting and degaussing must be periodically tested to verify complete erasure.

Crypto Erasure or Crypto Shredding must follow validated processes to ensure that cryptographic keys are protected from inadvertent deletion as well as ensure that keys are deleted when the storage is to be erased.

Disposal contractors must have appropriate personnel clearances, physical security of the facility, and procedures to store and handle the equipment and media (that may contain sensitive-enhanced or sensitive information) before and during disposal. Disposal contractors must be certified by the National Association of Information Destruction.

For locations associated with a District Office, computing equipment no longer needed for current operations must be sent to the District Office for disposal

through the USPS MDC Topeka in Topeka, Kansas (Address: 7215 S.W. Topeka Blvd., Bldg. 7, Topeka, KS 66624-9998). For locations not associated with a District Office, computing equipment no longer needed for current operations must be sent directly to the USPS MDC Topeka.

Hardware device disposal must be recorded in a Postal Service asset management system by the appropriate IT support organization.

3-5.8.2 Data Residue

As resources are allocated to data objects or released from those data objects (i.e., object reuse), information resources must have the capability to ensure that no accessible data is exposed to unauthorized users. Information resources must:

a. Have the capability to overwrite memory and storage that renders the information unrecoverable to prevent disclosure of sensitive-enhanced and sensitive information.

b. Restrict the capability to overwrite memory and storage to an authorized user.

c. Ensure that any previous information content of a resource is made unavailable upon the re-allocation of the resource for usage.

d. Ensure memory and storage allocated to processing sensitive-enhanced and sensitive information, including PCI transactions and authorization data is cleared before reallocation.

3-5.8.3 Non-electronic Information

Non-electronic information designated as sensitive-enhanced or sensitive must be destroyed by cross-cut shredding, pulping, or burning when no longer needed if the information is not subject to a legal hold and the retention period has expired.

Containers holding non-electronic information to be shredded must be constructed with suitable materials and a lock to prevent unauthorized access (e.g., a container similar to a mail collection box painted red).

3-5.9 Protection of Postal Service Information during International Travel

3-5.9.1 General Security Requirements While Traveling Outside of the United States

The transfer of files via portable storage devices, compact disks, and other file-sharing technology, exposes Postal Service systems to the possibility that information may be intentionally or inadvertently obtained by non-Postal Service personnel, or that malicious software may be transferred to Postal Service systems. Therefore, use of portable media and access to networks should be limited to only what is necessary for successful fulfillment of the international Postal Service mission and must be encrypted.

Any loss of devices suspected compromise or unusual computer activity must be reported to USPS CyberSafe *CyberSafe@usps.gov* before the computer is again connected to the Postal Service network.

Postal Service computers and mobile devices must not be taken outside of the United States on personal travel. Mobile devices are defined in 10-2.4 and 10-2.5.

Note: The Department of Homeland Security (DHS) may search, copy, and/or retain laptops, PDAs, USB devices, and other digital devices without cause at U.S. borders.

3-5.9.2 Substitution of Temporary Computer Equipment and Communication Devices

For some high-risk international destinations, users on official Postal Service business will be prohibited from traveling with their standard issue computers and mobile computing devices. In these instances, temporary equipment will be provided for the international mission by IT and the device will be wiped upon return.

3-5.10 Inclusion of Protection Requirements in Contracts

3-5.10.1 All Business Partners and Suppliers

Information security and privacy requirements must be included in all contracts involving Postal Service information.

The business partner or supplier must be compliant, at its own expense, with current federal legislation, federal regulations, federal directives, and industry requirements. To be enforceable, these requirements must be included in the contract. The Postal Service organization developing the requirements must either include them in the Statement of Work or work with the Contracting Officer to ensure such requirements are in the contract. The Postal Service or its designee may conduct audits of the business partner or supplier system and associated processes to assure compliance. In the event of noncompliance or a data breach, the business partner or supplier accepts full responsibility for all fines, lawsuits, and investigation and mitigation costs incurred by Postal Service resulting from such events.

3-5.10.2 Payment-Card Business Partners and Suppliers

Payment-card business partners and vendors must be compliant, at their own expense, with the Payment Card Industry (PCI) Data Security Standard (DSS), as amended or updated by the PCI Security Standards Council, and applicable to the Vendor Merchant or Service Provider Level as defined by the Visa Cardholder Information Security Program (CISP). The business partner or vendor is responsible for ensuring that its system performs each payment transaction in compliance with PCI-DSS requirements.

The Postal Service or its designee may conduct audits of the business partner or supplier payment systems and associated processes to assure PCI-DSS compliance. In the event of noncompliance or a data breach of the payment system or associated processes, the business partner or supplier accepts full responsibility for all fines, lawsuits, and investigation and mitigation costs incurred by the Postal Service resulting from such events. The business partner or supplier must accept these conditions in writing and provide a Letter of Attestation annually acknowledging their responsibility for the security of payment card data stored, processed, or transmitted on behalf of the Postal Service.

3-5.11 Additional PCI Requirements

PCI applications and cardholder information must reside on a restricted network segment or enclave on Postal Service premises. Cardholder information must not be stored off Postal Service premises on any device or media including hard drives, USB thumb drives, disks, diskettes, PDAs, smart phones, tablets, or laptops. Non-USPIS personnel may not send customer cardholder data (other than the first six and last four digits) via any electronic communication (including, but not limited to, email) for any reason, regardless of whether a USPS-approved encryption solution is utilized.

All PCI PANs must reside in a PCI approved enclave. All PCI PANs discovered outside the PCI enclave by the Data Loss Protection (DLP) program will be handled as follows:

a. The file will be moved to the DLP enclave and encrypted.
b. A marker file will be put in its place.
c. The owner will be notified when an owner can be determined.
d. The owner is responsible for remediation.

On the request of the OIG for forensics or the Privacy Office for notification of the cardholder or the card provider, the file will be stored encrypted in the DLP enclave until such time as the analysis or notification process is completed. At which time the file will be deleted.

3-5.12 Additional PII Requirements

All Social Security Numbers discovered on Postal Service information resources that are not encrypted by the Postal-approved encryption solution will be handled as follows:

a. The file will be moved to the DPL enclave and encrypted.
b. A marker file will be put in its place.
c. The owner will be notified when an owner can be determined.
d. The owner is responsible for remediation.

On the request of the OIG for forensics or the Privacy Office for notification of the individual, the file will be stored encrypted in the DLP enclave until the analysis or notification process is complete. At which time the file will be deleted.

IT must use approved encryption methods that can be discovered by security DLP tools.

3-5.13 Protection of Financial information

Applications that maintain inventories (e.g., supplies, merchandise, money orders, stamps, equipment) or financial information (e.g., accounts payable, accounts receivable) must implement appropriate controls to protect the integrity of the inventory/financial information and the application processes and to ensure individuals with access do not enrich themselves at the expense of the Postal Service. Possible controls that must be considered are input validation, separation of duties, audit logging, data retention, analysis of recipient addresses, check overprinting, control of check stock, and oversight of the printing and distribution process.

3-6 Protection of Non-Postal Service Information

3-6.1 Third-Party Information

Any information that does not belong to the Postal Service must be protected in accordance with legal requirements or contractual agreements with a third party except that when such requirements do not meet security standards for comparable Postal Service information, the Postal Service must meet or exceed its own standards.

3-6.2 National Security Classified Information

Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

3-7 Cyber Threat Information

Threat is any circumstance or event (human, physical, or environmental) with the potential to cause harm to an information resource in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting a vulnerability.

Cyber threats may include, but are not limited to, viruses, malware, Trojans, exploits, phishing attempts, and insider threats.

The objective of sharing cyber threat information is to support the overall CISO strategy and all information-sharing agreements, which must be approved by CISO leadership. The agreements must be coordinated with CISO units with a role in the collection, processing, storage, and protection of threat information.

An insider threat is a malicious or unintentional threat to an organization caused by the actions of a current or former employee, contractor, or business partner. Insider threats result from personnel exceeding or misusing their organizational access in a manner that affects the confidentiality, integrity, availability, or physical welfare of an organization's information, information systems, or workforce.

The Postal Service Insider Threat Program (InTP) works closely with the United States Postal Inspection Service (USPIS) and USPS Office of the Inspector General (OIG) to prevent, detect, and escalate instances of insider threat activity.

All threat information sharing must be managed within a Threat Intelligence Platform (TIP). The threat information-sharing process includes engaging in ongoing communication with partners, consuming security alerts and

indicators, organizing and storing information, and producing and publishing information for sharing with partners.

Threat information sharing must comply with Postal Service legal restrictions on the type of information that may be shared, including the requirement that shared threat information must not be attributable to the Postal Service.

Information types, such as Personally Identifiable Information (PII), classified information, and Postal Service proprietary information, may not be shared and must be protected. Adequate security and privacy controls must be implemented to protect this information from unauthorized disclosure or modification.

4 Security Risk Management

4-1 Policy

Risk assessments are required for all information resources, whether developed and operated in house or by business partners to ensure cost effective protection of information, applications, information resources, and the continuity of business operations. Site security reviews are also required for all facilities that house sensitive-enhanced, sensitive, or critical information resources, regardless of where they are located. Based on the results of risk assessments and site security reviews, managers must develop (or acquire) and implement security measures to handle unexpected events, avoid unacceptable losses, and minimize the effect of emergencies on business operations. Chapter 4 addresses the following:

a. Types of risk management.

b. Information resource risk management.

c. Independent risk management.

d. Site risk management.

All information resource risk management documentation must be treated as "restricted information" delivered to and retained by the executive sponsor with a copy to the Corporate Information Security Office to ensure all risk mitigation decisions are consolidated and appropriately made for like risks across Postal Service.

4-2 Types of Risk Management

The Postal Service implements the following three types of risk management:

a. Information resource risk management.

b. Independent risk management.

c. Site risk management.

4-3 Information Resource Risk Management

A risk assessment must be completed for all information resources. The risk assessment must address the following areas:

a. Identify the assets at risk and their value to the organization.

b. Identify the threats.

c. Identify the weaknesses and vulnerabilities.

d. Evaluate threats and vulnerabilities to determine the risks that threaten loss of value.

e. Identify possible safeguards (e.g., controls and countermeasures).

f. Analyze the costs and benefits of the safeguards in reducing the risks.

g. Complete the information resource risk assessment report.

The risk assessment must be completed in conjunction with system development. Additional risks may be identified in each of the life-cycle phases as development progresses through requirements definition, design, coding, testing, and production. The risks must be re-assessed and the risk assessment report updated as follows:

a. Every year for a payment card industry information resource.

b. After a significant audit finding.

c. Whenever the information resource experiences significant enhancement or modification, including changes to the infrastructure, operating system, or hardware platform.

d. After an information security incident that violates an explicit or implied security policy and compromises the integrity, availability, or confidentiality of an information resource.

e. Every 2 years for sensitive-enhance, sensitive, critical high and moderate, and externally facing information resources as part of the recertification process unless an earlier re-assessment is warranted.

f. Every 3 years for non-sensitive and noncritical information resources as part of the recertification process unless an earlier re-assessment is warranted.

Risks categorized as high or medium must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures. The risk mitigation process consists of the following:

a. Selecting the appropriate safeguards (or countermeasures) that will reduce exposure to the risk.

b. Assigning a priority ranking to the implementation of the safeguards.

c. Assigning financial and technical responsibility for implementing the safeguards.

d. Implementing and documenting the safeguards.

e. Maintaining the continued effectiveness of the mitigation strategy by reassessing the threats, vulnerabilities, effectiveness of the safeguards, and the residual risk.

If the level of residual risk is not acceptable, then further safeguards and security controls should be implemented to reduce exposure to acceptable levels. The vice president of the functional business area is responsible for accepting (and the vice president, Information Technology Solutions is

responsible for acknowledging), in writing, the residual risks inherent with using that information resource or initiating steps to further mitigate the residual risk.

All information resource risk management documentation must be treated as "restricted information" delivered to and retained by the executive sponsor and a copy sent to the Corporate Information Security Office.

4-4 Independent Risk Management

An independent information risk assessment may be required during the business impact assessment process. Independent risk assessments are conducted by organizations that are separate and distinct from those responsible for the development and operation of the information resources. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for the criteria for conducting an independent risk assessment.)

4-5 Site Risk Management

A site security review must be performed for each site hosting sensitive-enhanced, sensitive, or critical information resources and may be required for business partner and vendor sites requesting connectivity to the Postal Service intranet to:

a. Identify the location of the facility and structure-specific strengths and weaknesses.

b. Identify the sensitive-enhanced, sensitive, and critical information resources hosted by that facility.

c. Identify the threat events that could occur, including physical threats (e.g., power failure, fire, building collapse, water damage from plumbing failure and roof leak); environmental threats (e.g., earthquake, flooding, tornadoes, lightning, and sink hole); and human threats (e.g., union lockouts, riot, disgruntled employee or customer, and armed theft).

d. Evaluate threats and vulnerabilities to determine the frequency and amount of harm that could possibly occur as a result of a physical, environmental, or human event.

e. Identify possible additional administrative, technical, and physical security safeguards.

f. Analyze the costs and benefits of the safeguards in reducing the risks.

A site security review is conducted at the following times:

a. Before a new site becomes operational.

b. After significant changes at the site, including significant changes in information resources located there.

c. Every 3 years, unless an earlier site security review is warranted.

Risks categorized as high must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures. The risk mitigation process consists of the following:

a. Selecting the appropriate safeguards (or countermeasures) that will reduce exposure to the risk.

b. Assigning a priority ranking to the implementation of the safeguards.

c. Assigning financial and technical responsibility for implementing the safeguards.

d. Implementing and documenting the safeguards.

e. Maintaining the continued effectiveness of the mitigation strategy by reassessing the threats, vulnerabilities, effectiveness of the safeguards, and the residual risk.

If the level of residual risk is not acceptable, then further safeguards and security controls should be implemented to reduce exposure to acceptable levels. The installation head is responsible for acknowledging and accepting the residual site risk.

The site security review will be performed by the manager CISO and the Chief Inspector or their designees. All site risk management documentation must be treated as "restricted information" and delivered to and retained by the Inspection Service and the appropriate installation head.

4-6 Risk-Based Information Security Framework

The risk-based information security framework [1] allows traceability from the highest-level strategic goals and objectives of the Postal Service, through specific mission/business protection needs, down to specific information security solutions and [2] incorporates information security requirements from legislation, directives, policies, regulations, standards, and guidance.

A risk-based strategy gives vice presidents of functional business areas, executive sponsors, and Business Relationship Management portfolio managers the opportunity to make informed risk-based decisions in dynamic operating environments—decisions based on trade-offs between fulfilling business functions and managing the many types and sources of risk that must be considered. Information security risks must be aligned with business risks to accurately gauge the effectiveness of information security controls.

The following key elements are required to effectively manage information security risks for the Postal Service:

- Assignment of risk management responsibilities to vice presidents of functional business areas, executive sponsors, and Business Relationship Management portfolio managers.

- Recognition and acceptance of the information security risks to Postal Service information resources, individuals, and other organizations (e.g., business partners, vendors, customers) arising from the operation and use of information systems.
- Establishing the tolerance for risk and communicating the risk tolerance throughout the Postal Service, including guidance on how risk tolerance impacts ongoing decision-making activities and the overall security stance of the Postal Service, not just to a specific information resource, process, or organization.
- Accountability by vice presidents of functional business areas, executive sponsors, and Business Relationship Management portfolio managers for their risk management decisions.

5 Acceptable Use

5-1 Policy

Postal Service information resources must be used in an approved, ethical, and lawful manner to avoid loss or damage to Postal Service operations, image, or financial interests and are used to comply with official policies and procedures on acceptable use. Personnel must contact the manager, Corporate Information Security Office, prior to engaging in any activities not explicitly covered by the following policies:

a. Personal use of government office equipment including information technology.

b. Electronic mail and messaging.

c. Internet.

d. Prohibited uses of information resources.

e. Protection of sensitive personal and Postal Service information.

All Postal systems (on premise, hosted, cloud) must display or provide a link to notify users of the Postal Service terms of use and privacy notice.

5-2 Personal Use of Government Office Equipment Including Information Technology

Management at each Postal Service facility may permit employees to make limited personal use of Postal Service office equipment, including information technology equipment, provided such use does not reduce or otherwise adversely affect the employee's productivity during work hours, does not interfere with the mission or operations of the Postal Service, and does not violate the Standards of Ethical Conduct.

The office equipment governed by this policy includes, but is not limited to, personal computers; personal digital assistants (including Blackberries); peripherals, such as printers and modems; computer software (including Web browsers); telephones; cell phones; smart phones; tablets; smart watches; facsimile machines; photocopiers; scanners; label writers; consumable office products; office supplies; removable media; library resources; Internet connectivity; remote-access technologies (e.g., VPN);

and e-mail. Use of Postal Service information resources constitutes permission to monitor that use.

Limited personal use of Postal Service office equipment, including information technology, means occasional use that meets the following criteria:

a. Is of limited duration, length, or size, and does not interfere with employees' official duties or the transaction of official Postal Service business.

b. Results in only minimal, if any, additional expense to the Postal Service or minimal wear and tear on Postal Service office equipment; uses a small amount of data storage; has only a small-to-moderate transmission impact; or requires only small amounts of consumable office products (e.g., ink, paper, toner, and computer memory).

Some examples of limited personal use are:

a. Making a few photocopies.

b. Make occasional, brief telephone calls that result in little or no cost.

c. Sending an occasional facsimile of a few pages.Sending a brief personal email message that contains only text (no urls, files, or images attached).

d. Doing a brief Internet search.

Limited personal use of Postal Service office equipment, including information technology, must not:

a. Reduce employee productivity or interfere with official Postal Service business (e.g., congest, delay, or disrupt any Postal Service system or equipment).

b. Be for the purpose of maintaining or promoting a personal or private business.

c. Be for the purpose of posting unauthorized commercial or advertising materials.

d. Be for any illegal purpose, including, but not limited to, gaining unauthorized access to other systems; disseminating any discriminatory or hate-based materials or speech; or reproducing or distributing copyrighted, trademarked, proprietary, or export-controlled data or software.

e. Be in relation to sexually explicit or sexually oriented materials.

f. Refer or relate to illegal gambling, illegal weapons, and/or terrorist activities.

g. Be for the purpose of fundraising, endorsing any product or service, lobbying, or participating in any prohibited partisan political activity.

h. Be for the purpose of using applications and/or software that have not been approved by the Postal Service and that occupy or impact official computer or network processing time.

i. Result in the disclosure of any Postal Service information that is not otherwise public.

Use of Postal Service office equipment in violation or excess of the limited personal use permitted by this policy may result in limitations on future use, administrative action, criminal penalty, and personal financial liability.

For advice on how to avoid violating this policy and the corresponding misuse of government property prohibitions in the Standards of Ethical Conduct, please call the Postal Service's Ethics Helpline at 202-268-6346 or send an e-mail to *ethics.help@usps.gov*.

5-3 Electronic Mail and Messaging

Access to the Postal Service electronic mail (e-mail) system is provided to personnel whose duties require e-mail to conduct Postal Service business. If you do not comply with Postal Service e-mail policies your e-mail account may be disabled and you will have to request your manager apply to the manager, CISO, for reinstatement of the lost privileges. Only Postal Service provided e-mail services may be accessed from Postal Service information resources. Since e-mail may be monitored, anyone using Postal Service resources to transmit or receive e-mail should have no expectation of privacy.

Sensitive-enhanced and sensitive information must be sent only to authorized personnel with a need to know and must be encrypted. Unprotected payment card industry (PCI) primary account numbers (PANs) are not to be sent via end-user messaging technology, including e-mail, chat, instant messaging, etc.

Although occasional and incidental personal e-mail use is permitted, personal messages while they remain in the system will be considered to be in the possession and control of the Postal Service.

5-3.1 Prohibited Use

Do not use Postal Service provided computing devices, including mobile devices, to check non-Postal Service (e.g., personal, supplier, contractor, and vendor) e-mail accounts (e.g., Hotmail, Yahoo, Excite, MSN) or social media. Do not use personal electronic devices to receive, process, store, or send mail containing Postal Service sensitive-enhanced, sensitive, or non-publicly available information. Other prohibited activities when using Postal Service e-mail include, but are not limited to, sending or arranging to receive the following:

a. Information that violates state or federal laws or Postal Service regulations.

b. Information designated as sensitive-enhanced or sensitive information unless encrypted according to Postal Service standards.

c. Unsolicited commercial announcements or advertising material.

d. Any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the Postal Service, the recipient, the sender, or any other person.

e. Pornographic, sexually explicit, or sexually oriented material.

f. Racist, hate-based, or offensive material.

g. Viruses or malicious code.

h. Chain letters, unauthorized mass mailings, or any unauthorized request that asks the recipient to forward the message to other people.

5-3.2 Encryption

Encrypting e-mail or messages must comply with the following:

a. Encryption software and methods must be approved by the Enterprise Architecture Committee.

b. Encryption solutions must either support key recovery or keys must be registered with authorized personnel.

c. Recovery keys or other similar files for all encrypted e-mail must be placed in a directory or file system that can be accessed by management prior to encrypting e-mail.

d. Recovery keys or other devices needed to decrypt e-mail must be provided when requested by authorized Postal Service management, the Postal Inspection Service or the Office of Inspector General.

e. Keys may not be escrowed in customer product offerings unless specifically requested in writing by the customer and approved by the executive sponsor.

5-4 Internet: Access and Prohibited Activities

Access to the Internet is available to employees, contractors, suppliers, and business partners whose duties require access to conduct Postal Service business. Since Internet activities may be monitored, all personnel accessing the Internet will have no expectation of privacy.

Prohibited activities when using the Internet include, but are not limited to, the following:

a. Downloading unauthorized content and accessing information resources outside of the Postal Service network; this includes but is not limited to using a VPN connection or attempting to bypass any Postal Service approved access technologies.

b. Browsing explicit pornographic or hate-based Web sites, hacker or cracker sites, or other sites that the Postal Service has determined to be off limits.

c. Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material the Postal Service has determined to be off limits.

d. Posting or sending sensitive-enhanced or sensitive information outside of the Postal Service without management authorization.

e. Hacking or other unauthorized use of services available on the Internet.

f. Posting unauthorized commercial announcements or advertising material.

g. Promoting or maintaining a personal or private business.

h. Receiving news feeds, push data updates, or continuous data streams unless the material is required for Postal Service business.

i. Using non-Postal Service-approved applications or software that occupy or use workstation idle cycles or network processing time (e.g., processing in conjunction with screen savers).

5-5 Prohibited Uses of Information Resources

Generally prohibited activities when using information resources include, but are not limited to, the following:

a. Stealing electronic files containing nonpublic information or copying, moving, or storing electronic files containing nonpublic information to local hard drives, removable media, or via remote-access technologies.

b. Violating copyright laws.

c. Installing unauthorized software, including games and screen savers.

d. Browsing the private files or accounts of others, except as provided by appropriate authority.

e. Performing unofficial activities that may degrade the performance of information resources, such as playing electronic games.

f. Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, and decrypt encrypted files, or compromise information security by any other means.

g. Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of, or access to, any Postal Service computer, network, or information.

h. Accessing the Postal Service network via modem or other remote access service without the approval of the manager, Corporate Information Security Office Information Security Services.

i. Promoting or maintaining a personal or private business or using Postal Service information resources for personal gain.

j. Conducting fraudulent or illegal activities including, but not limited to, gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any Postal Service or non-Postal Service computer.

k. Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.

l. Disclosing any Postal Service information that is proprietary and not otherwise public without authorized management approval.

m. Performing any act that may defame, libel or misrepresent the Postal Service, its personnel, business partners, or customers.

n. Using someone else's log-on ID and password or any other personal identity credential.

o. Using personal information resources (e.g., laptops, notebooks, personal digital assistants [PDAs], hand-held computers, or storage media including universal serial bus [USB] devices) at retail counter areas, mail processing areas, or workroom floors. This does not apply to personal information resources used by the unions in accordance with the collective bargaining agreement.

p. Connecting any non-Postal Service (e.g. personal, contractor, or supplier) information resources to the Postal Service intranet (Blue) or Postal Service computing devices.

q. The physical or wireless connection of personal mobile computing devices, such as cell phone, smart phones, tablets, and other mobile computing devices of any kind (excluding laptops) to any Postal Service network, regardless of purpose, is strictly prohibited under any circumstances.

r. Using non-Postal Service (e.g., personal, contractor, supplier) information resources to collect, process, store, transmit Postal Service sensitive-enhanced, sensitive, or non-publicly available information.

s. Plugging a Postal Service non-encrypted USB drive into a personal computing device.

t. Using unauthorized webcams, cameras, cell phones with cameras, or watches with cameras (and other personal imaging devices) in restrooms, locker rooms, retail counter areas, mail processing areas, workroom floors, vehicles, or other Postal Service areas unless approved by area or headquarters vice president or designee for business purposes. (See Management Instruction AS882-2007-6, *Postal Service Use of Retail and Cell-Phone Cameras,* on the use of handheld and cell phone cameras.)

u. Sending unprotected PANs.

v. Copying, moving, or storing cardholder data onto local hard drives or removable media when accessing cardholder information via remote access technologies.

5-6 Protection of Sensitive Data and Privacy-Related Data

Information resources must protect Postal Service sensitive data and the privacy-related data of customers, employees, and contractors in accordance with the Postal Service privacy policy and the Privacy Act as applicable. Postal Service policies related to privacy, the Freedom of Information Act, and records management can be found in Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management.* The Postal Service privacy policy for customers is posted on *www.usps.com.*

5-7 Sensitive Data Storage

Postal Service limits storing sensitive data to explicit business requirements. Personally Identifiable Information (PII) is prohibited from being stored for any longer than the legitimate business need exists to retain the data. Customer credit card numbers or Primary Account Numbers (PANs) should be rendered unreadable at-rest in compliance with the PCI DSS.

Supplemental Guidance: Postal Service is not required to storage of customer data for credit or debit cardholders and sensitive authentication data, after transaction authorization, is prohibited, in any form, even if it is encrypted. This includes the following data elements:

a. The full contents of any track from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere.

b. The card verification code or value three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions

c. The personal identification number (PIN) or the encrypted PIN block.

d. In the normal course of business, the following data elements from the magnetic stripe may need to be retained to minimize risk. Store only these data elements as needed for business:

1. The cardholder's name
2. Primary account number (PAN)
3. Expiration date
4. Service code

5-8Use of Social Media

The *Administrative Support Manual* (ASM), 363, Social Media Policy, governs the use of social media by Postal Service employees and contractors when serving the Postal Service in an official or professional capacity and provides rules and guidance for Postal Service employees and contractors who use social media for personal purposes.

6 Personnel Security

6-1 Policy

The Postal Service identifies sensitive positions and ensures that individuals assigned to those positions have the appropriate level of clearance to minimize risk to Postal Service information resources.

Personnel are held accountable for carrying out their information security responsibilities. Managers must ensure personnel receive appropriate information security training and protect Postal Service resources when personnel depart under involuntary or adverse conditions.

Policies addressed in this chapter are the following:

a. Employee accountability.

b. Sensitive positions.

c. Background investigations and clearances.

d. Information security awareness and training.

e. Departing personnel.

6-2 Employee Accountability

6-2.1 Separation of Duties and Responsibilities

Personnel must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud, or collusion.

6-2.2 Job Descriptions

The Postal Service defines and documents the information security requirements for each position.

6-2.3 Performance Appraisals

The Postal Service evaluates the execution of information security responsibilities and the compliance with information security policies and procedures in personnel performance appraisals.

6-2.4 Condition of Continued Employment

The Postal Service includes the execution of information security responsibilities and the compliance with information security policies and procedures as a condition of continued employment for all personnel.

6-2.5 Sanctions

All personnel are held accountable for carrying out their information security responsibilities. Violators of Postal Service information security policies are subject to sanctions by supervision commensurate with the severity and frequency of the infraction, including levels of access, disciplinary action, removal, or criminal prosecution.

6-3 Sensitive Positions

Managers at all levels are responsible for identifying sensitive positions within their organizations and then requesting the chief postal inspector to designate the positions as sensitive.

Sensitive positions include those in which personnel could, in the normal performance of their duties, cause material adverse effect to Postal Service information resources. Such duties include, but are not limited to, the following:

a. Making changes in the operating system, configuration parameters, system controls, and audit trails.

b. Modifying security authorizations.

c. Making revisions to sensitive programs and data that could be undetected.

6-4 Background Investigations and Clearances

6-4.1 General Requirements

Personnel must have appropriate background investigations/security clearances as determined by the Postal Inspection Service before accessing Postal Service information resources (see ASM 272, Personnel Security Clearances). For personnel without clearances, access is restricted to temporary information services (see 9-3.2.2, Temporary Information Services).

Appropriate background investigations must be conducted and security clearances obtained for personnel who access sensitive-enhanced, sensitive, or critical information resources, require unescorted access to controlled areas, or perform the duties of a sensitive position.

Personnel includes employees, nonemployees, business partners, and suppliers having access to Postal Service sensitive-enhanced or sensitive data whether that data is stored on Postal Service premises or at a business partner, supplier, or vendor facility.

6-4.2 Access Privileges

6-4.2.1 Log-on IDs

Managers must use eAccess/ARIS to request access authorization for individuals who do not have the appropriate clearance or background investigation and are responsible for the access activities of those individuals.

6-4.2.2 Information Resources Processing Sensitive - Enhances or Sensitive Information

All personnel whose duties require access to Postal Service information resources processing sensitive-enhanced or sensitive information (see 3-2, Information Designation and Categorization) must have an appropriate clearance or background investigation as determined by the Inspection Service before they obtain access (see ASM 272, Personnel Security Clearances).

6-4.2.3 Controlled Areas

All personnel, whose duties require unescorted access to controlled areas, whether located at a Postal or non-Postal Service facility, must have an appropriate clearance or background investigation as determined by the Inspection Service before being granted unescorted access privileges. For further information, refer to the USPS *Administrative Support Manual* (ASM), Section 272, Personnel Security Clearances.

6-4.3 Foreign Nationals

In certain situations, personnel may be permanent resident aliens and citizens of foreign countries and still provide services to the Postal Service, with prior approval of the responsible executive. Except for citizenship, foreign nationals must meet the same clearance requirements as all other personnel. The Postal Service executive who approves access to information resources by foreign nationals (including contractors and suppliers) is responsible for all actions initiated by the foreign national.

6-5 Information Security Awareness and Training

6-5.1 General Security Awareness

Managers must continually strive to incorporate information security into training courses, training videos, service talks, internal newsletters, posters, case studies, and other tools and visual aids to increase information security awareness among their personnel. The training should explain how anyone failing to comply with security policies and procedures will be disciplined.

6-5.2 Documenting and Monitoring Individual Information Security Training

Individual information security training activities must be documented and monitored to ensure all personnel attend their initial, annual, and operational training (as required) before given access to sensitive-enhanced, sensitive, or critical information.

If Postal Service-sponsored training is not available, contractors must provide appropriate information security training that is applicable to the Postal Service computing environment.

All designated personnel (see the Information Security Training Matrix on the CISO Website for the current requirements) handling PCI information must acknowledge, at least annually, in writing or electronically, that they have read and understand Postal Service information security policies and procedures contained in Handbook AS-805-C, *Information Security for General Users,* as well as the security procedures associated with their job.

6-5.3 Training Requirements

Exhibit 6-5.3

Training Requirements

Training Type	Requirement(s)
Annual Training	Based on requirements defined by the CISO at the beginning of the fiscal year (see the Information Security Training Matrix on the CISO Website), all personnel with an ACE ID or access to the Postal Service intranet must participate in information security training and data protection requirement training annually. Information security training is recommended for all other non-bargaining personnel.
Information Resource Operational Security Training	All personnel with access to the Postal Service network must be trained to handle and report information security breaches and incidents. All developers and administrators must complete formal training [1] in general secure coding techniques, [2] in developing secure code in the programming language(s) they use, and [3] and must maintain evidence of successful completion. For information resources processing sensitive-enhanced, sensitive, or critical information, operational security training must be developed and conducted that is appropriate for job responsibilities, and role-based activities. All privileged users posing access to any sensitive-enhanced, sensitive, or critical information or systems supporting information must undergo security awareness training and records are maintained within the Learning Management System (LMS). If training does not occur, the role cannot be fulfilled. For privileged account holders who have not received annual refresher training, access is disabled until required training has been completed, unless the CISO grants a waiver. The training should explain how to protect information throughout its life cycle and report incidents. All C&A stakeholders, including Business Relationship Management portfolio managers, Solution Development Teams, and their staff must complete annual training on the Certification and Accreditation (C&A) process.

New Personnel Training	All new personnel must receive information security training and be issued a copy of Handbook AS-805-C, *Information Security for General Users.*

6-6 Departing Personnel

6-6.1 Routine Separation

Routine separation of personnel occurs when an individual receives reassignment or promotion, resigns, retires, or otherwise departs under honorable and friendly conditions. Unless adverse circumstances are known or suspected, the individual will be permitted to complete his or her assigned duties and follow official employee departure procedures. When personnel leave under non-adverse circumstances, the individual's manager, supervisor, or company official (for contractors/suppliers) must ensure the following:

a. All accountable items, including keys, access cards, two-factor credentials, laptops, tablet computers, mobile computing devices (including smart phones and encrypted storage devices) and other computer-related equipment are returned.
b. For Postal Service employee's, the employee computer log-on ID, building-access authorizations, and access to Postal Service information systems are terminated coincident with the employee's effective date of departure determined by Human Resources, unless needed in the new assignment.
c. For contractors and suppliers, their individual computer log-on ID, building-access authorizations, and access to Postal Service information systems are terminated immediately with their date of departure.
d. All sensitive-enhanced and sensitive information, in any format, in the custody of the terminating individual are returned, destroyed, or transferred to the custody of another individual.

6-6.2 Adverse Termination

Removal or dismissal of personnel under involuntary or adverse conditions includes termination for cause, involuntary transfer, and departure with pending grievances. In addition to the routine separation procedures, termination under adverse conditions requires extra precautions to protect Postal Service information resources and property. The manager, supervisor, or company official (for contractors/suppliers) of an individual being terminated under adverse circumstances must:

For Postal Service employees:

a. Ensure that the individual is escorted and supervised at all times while in any location that provides access to Postal Service information resources.
b. Immediately suspend and take steps to terminate the individual's computer log-on ID(s), access to Postal Service information systems, and building access authorizations.
c. Ensure prompt changing of all computer passwords, access codes, badge reader programming, and physical locks used by the individual

being dismissed.

d. Attempt to recover accountable items and all sensitive-enhanced and sensitive information in any format in the custody of the individual being terminated.
e. Attempt to wipe and/or lock any accountable item that cannot be recovered.
f. Destroy or transfer sensitive-enhanced or sensitive information to another custodian.
g. Notify the Postal Inspection Service.

Contractors and Suppliers:

a. Ensure immediate deletion of all computer passwords, access codes, badge reader programming, and physical locks used by the individual being dismissed.
b. Recover accountable items and all sensitive-enhanced and sensitive information in any format in the custody of the individual being terminated.
c. Wipe and/or lock any accountable item that cannot be recovered.
d. Destroy or transfer sensitive-enhanced or sensitive information to another custodian.
e. Immediately notify the contractor's and/or supplier's program manager (PM) or contract officer representative (COR).
f. Ensure the Contractors/Suppliers eAccess/ARIS account is terminated.
g. Before escorting the individual off the premises secure the Postal Service badge/ID.

6-6.3 Systems, Network, or Database Administrator Departure

Routine separation or adverse termination of a systems, network, or database administrator requires taking extra care and precautions. Upon departure, remove the privileged access as quickly as possible to maintain the security and integrity of the specific information resources to which the administrator had access. After departure, monitor the affected information resources for improper use or access. Specifically, the manager, supervisor, or company official (for contractors/suppliers) of the departing systems or database administrator must:

a. Follow the requirements documented above for routine separation or for adverse termination as applicable.
b. Reconfigure access lists to remove the departed administrator's accounts.
c. Disable or change the password or login requirements to all shared devices and applications.
d. Disable or change passwords to all shared service and privileged accounts.
e. Disallow physical access to buildings, systems, and information associated with the departed administrator's former access.
f. Monitor all privileged accounts for usage and access to the systems, applications, and databases formerly under the administrator's control to ensure all access has been removed.

g. Review records for Postal Service information approved for removal offsite and make appropriate efforts to recover information and/or equipment as applicable. Notify the manager, Corporate Information Security Office, of any information identified as removed but not recovered.

7 Physical and Environmental Security

7-1 Policy

The Postal Service protects its information resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorized personnel.

Where possible, all information resources (including portable information resources) must reside in a protected environment. Physical and administrative security controls must be implemented at each facility to protect against unauthorized personnel access and to protect the physical integrity of Postal Service information resources located at the facility. Such physical and administrative security controls include the following:

a. Physical access controls.

b. Physical protection of information resources.

c. Environmental security.

d. Facility continuity planning.

e. Facility contracts.

7-2 Physical Access Controls

7-2.1 Access to Controlled Areas

Access to controlled areas must be restricted as follows:

a. Access to controlled areas is restricted to personnel whose duties require access to such facilities and who possess appropriate security clearances or background investigation.

b. Access to controlled areas must be controlled by electromechanical means. Personnel authorized access to the controlled areas must always use their access control identification badge or device to gain entrance to the controlled area. Tailgating is prohibited and personnel are responsible for immediately reporting any instance of tailgating.

c. A record of physical access, both authorized individuals and visitors, must be maintained. Automated mechanisms should be employed where feasible to facilitate the maintenance and review of access records.

d. Personnel without an authorized Postal Service identification badge or device must sign a visitor log and be escorted by authorized personnel while in the controlled area.

e. Visitor logs must include at a minimum: name and organization of the person visiting, form of identification used for authentication, date of visit, time of entry and departure, purpose of visit, and name of person and organization visited. Visitor logs must be reviewed monthly and security violations and suspicious activities must be investigated and remedial actions taken.

7-2.2 Establishment of Controlled Areas

Controlled areas must be established within the facility wherever more stringent restrictions on physical access and more tightly controlled physical and environmental security are required to fully protect information resources. Typical controlled areas may include the following:

a. Computer rooms.

b. Telecommunications rooms.

c. Wiring closets.

d. Computer operations areas.

e. Media and documentation storage areas.

f. Operating system software support areas.

g. Special authorization terminal areas.

h. Security officers' controlled areas.

i. Other designated areas, whether located at a Postal Service or non-Postal Service facility.

7-2.3 Types of Information Resources Stored in Controlled Areas

Information resources processing sensitive-enhanced, sensitive, or critical information must be located in a controlled area.

7-2.4 Establishment of Access Control Lists

Each controlled area must establish an access control list of people who are authorized access. Access control lists must be updated when new personnel are assigned to the controlled area or when someone leaves. Access control lists must also be reviewed and updated semiannually. Data center access must be reviewed by the designated Information Technology manager on a quarterly basis.

Personnel not on the access control list must sign a visitor log and be escorted by authorized personnel while in the controlled area.

7-2.5 Training for Controlled Areas

Personnel with access to controlled areas must be trained in their responsibilities regarding controlled areas.

7-2.6 Installation of Physical Access Control Devices

Physical access control devices using biometrics, smart cards, tokens, mantraps, or lockable cabinets may be installed to supplement traditional facility locks and keys to limit access. Additionally, the Inspection Service and Facility Management may require physical access to be monitored by surveillance equipment and real time intrusion detection and alarm systems (e.g., CCTV, motion detectors, and other audio or silent alarms) to detect and respond to incidents [see the *Administrative Support Manual* (ASM) 273, Facility Security, and Handbook RE-5, *Building and Site Security Management*].

Based on the risks associated with the information resource, additional physical access security mechanisms (e.g., locked cabinet or desk, portable device cable lock, and biometric workstation lock) must be implemented for information resources processing sensitive-enhanced, sensitive, or critical information.

Security personnel are notified immediately of physical security events and follow-up action is taken and documented.

7-2.7 Implementation of Identification Badges

Identification badges must adhere to the following criteria:

a. Persons authorized access to controlled areas must be identified by a picture badge conspicuously displayed on their person.

b. Persons using a badge not issued to them or making any attempt to alter a badge will be subject to disciplinary action.

c. Employees must report lost or stolen badges immediately to the issuer of the badge.

d. Security access systems that limit access to controlled areas where persons have reported lost or stolen badges must immediately cancel the associated access privileges until the lost or stolen badge is recovered and returned to the issuer.

e. Temporary badges must be controlled and issued by the manager of the organization or their designee to authorized personnel who arrive without their assigned badges during normal duty hours.

f. The organization manager or designee must make an unannounced verification of badges at least annually to ensure authenticity and to correct any badge discrepancies.

7-3 Physical Protection of Information Resources

Information resources must be protected against damage, unauthorized access, and theft, both in the Postal Service environment and when removed from this secure environment.

Note: Sensitive-enhanced, sensitive, and critical information stored on removable devices or media must be encrypted and stored in a controlled area or in a locked cabinet. Sensitive-enhanced and sensitive information that is stored off Postal Service premises must also be encrypted and stored in a controlled area or in a locked cabinet.

7-3.1 Network Equipment, Network Servers, and Mainframes

Network equipment, network servers, and mainframes must be protected against damage, unauthorized access, and theft and, where possible, housed in separate rooms that can be accessed only by authorized personnel.

Additional protection measures to control physical access to information distribution and transmission include locked wiring closets, disconnected or locked spare jacks, and protection of cabling with conduit or cable trays.

7-3.2 Postal Service Workstations and Portable Devices

Postal Service information resources that are stationary, portable, or mobile must be protected at all times in use, storage, and in transit against damage, unauthorized access, and theft. Users of Postal Service information resources will be held accountable for their loss or compromise.

7-3.3 Non-Postal Service Portable Electronic Devices

To protect Postal Service information from disclosure or compromise, non-Postal Service portable devices [e.g., laptops, notebooks, tablets, mobile computing devices, or storage media including universal serial bus (USB) port devices or thumb drives] must not store, process, or transmit Postal Service information. Under no circumstances will such devices connect to the Postal Service intranet via a wired or wireless connection.

The use of non-Postal Service portable devices for personal use is controlled by rules set forth by the installation head or his or her designee.

Visitors to Postal Service facilities may be required to present non-Postal Service portable devices to the installation head or his or her designee upon entry to the facility. The installation head or his or her designee determines if such devices can be brought into the facility or must be surrendered for the duration of the visit. Under no circumstances will such devices connect to the Postal Service intranet or store, process, or transmit Postal Service information.

7-3.4 Sensitive-Enhanced, Sensitive, and Critical Media

Sensitive-enhanced, sensitive, and critical media, whether electronic or non-electronic, must be protected against physical loss or damage, whether on Postal Service premises or not. Physical and administrative controls must be implemented to ensure that only authorized personnel can access sensitive-enhanced, sensitive, and critical information. Personnel who have custody of sensitive-enhanced, sensitive, and critical media are responsible for their safekeeping (see 3-5, Protection of Postal Service Information and Media).

7-3.5 Contracts

Physical security requirements must be included in contracts involving infrastructure services performed or hosted for the Postal Service.

7-4 Environmental Security

Environmental security controls must be implemented at the facility, room, and information resource level to protect servers, mainframes, and critical information resources as described below:

a. Protection against lightning, wind, and building collapse must be implemented.

b. Protection against water damage from water supply lines, sewer systems, and roof leaks must be implemented (e.g., plastic sheets are available and master shutoff valves are accessible, working properly, known to operations personnel, and automatic where feasible).

c. Additional temperature and humidity safeguards must be implemented to monitor and maintain acceptable levels.

d. Protection against flooding, earthquakes, or other natural disasters must be implemented (e.g., drains are installed below the computer room floor).

e. Additional fire safeguards:

   (1) Fire detection and suppression equipment (e.g., smoke and heat detectors, handheld fire extinguishers, fixed fire hoses, and sprinkler systems) must be implemented.

   (2) Fire detection and suppression equipment must automatically notify the organization and emergency responders.

f. Additional power (electricity) safeguards:

   (1) A short-term alternate power supply must be implemented to ensure proper shutdown in the event of a power interruption.

   (2) A long-term alternate power supply must be implemented to maintain minimal operational capability in the event of a power outage.

g. Automatic emergency lighting systems must be implemented to illuminate emergency exits and evacuation routes in the event of a power outage or disruption.

h. Surge protection must be implemented for all information resources.

i. Redundant power feeds and redundant communications paths must be implemented for critical information technology sites.

For areas containing concentrated information resources, Facility Management may require the capability to shut off power to information resources that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to potential flooding) without endangering personnel by requiring them to approach the equipment. See ASM 273, Facility Security, and Handbook RE-5, *Building and Site Security Management,* for the requirements for remote power shutoffs.

7-5 Facility Continuity Planning

Physical security requirements must be included in facility continuity planning to ensure the appropriate protection of information resources following a catastrophic event.

7-6 Facility Contracts

Depending on the nature of the contract, information, environmental, personnel, and physical security requirements must be included in contracts involving facilities to ensure the appropriate protection of information resources.

8 Development and Operations Security

8-1 Policy

Information resources must be developed under the technical solutions life cycle (TSLC) or other approved system development life cycle methodology. Information security must be an integral part of the system development life cycle whether development is done in house, acquired, or outsourced. Postal Service information must also be appropriately protected during operation. Security activities must be performed to maintain a secure environment and to comply with Postal Service policies and legal requirements.

The Postal Service certification and accreditation (C&A) process defines a formal review process that ensures adequate security is incorporated during each phase of the project life cycle. The C&A process is required for each information resource (i.e., application or infrastructure component).

Chapter 8 addresses the following topics:

a. Development security.

b. Operations security.

c. Certification and accreditation.

8-2 Development Security

8-2.1 Life-Cycle Approach

Security must be addressed throughout the information resource life-cycle process, from requirements, design, build, system integration testing (SIT), customer acceptance testing (CAT), release (and production) and retirement. All development, acquisition, or integration projects for information resources,

whether performed in house or by a business partner, must follow the TSLC process or other approved systems development life-cycle methodology. All systems development must follow secure coding best practices.

8-2.2 Risk Management

A risk-based approach must be applied to information security that uses limited resources wisely to protect an information resource in a cost-effective manner throughout its life cycle. The security controls applied to information resources must be commensurate with the magnitude of harm that would result from loss, misuse, unavailability, unauthorized access, or unauthorized modification of the information resources (see 4-3, Information Resource Risk Management).

8-2.3 Quality Assurance

Information resource development must include quality assurance (QA) and security-specific testing to ensure that security controls have been implemented and are functioning correctly. Transactions failing edit and validation routines must be subject to appropriate follow-up until errors are remediated. Information processing failures discovered as the result of remediation must be used for root cause analysis and to adjust procedures and automated controls to improve quality.

8-2.4 Configuration and Change Management

All information resources, whether developed in house, outsourced, or acquired must be developed under standard configuration and change management procedures to maximize risk reduction and vulnerabilities introduced by undocumented and untested changes in accordance with the Postal Service change management policy/procedure. Postal Service information resources must not be developed or deployed unless a change and configuration management process is in place.

Configuration and change control involve the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. Appropriate organizational officials approve information system changes in accordance with this process. Emergency changes are also included in the configuration and change control process.

8-2.4.1 Configuration Component Inventory

To effectively manage information resources, the information system components must be inventoried and the initial or baseline configuration of the information resources must be documented in the corporate Configuration Management Database (CMDB) prior to deployment. The inventory of information system components must include manufacturer, type, serial number, version number, information system/component owner, and location (i.e., physical location and logical position within the information system architecture). The inventory must also designate those information system components required to implement and/or conduct contingency planning operations.

Configurations of information resources must be reviewed at least annually to ensure the documented configuration in the appropriate inventory application matches the current components.

8-2.4.2 Configuration Hardening Standards

Hardware and system software must be hardened to Postal Service information security requirements. Configuration hardening standards must be used to maintain a high level of information security, enable cost-effective and timely maintenance and repair, and protect Postal Service information resources against unexpected vulnerabilities. Critical security patches for PCI-related information resources, including applications and infrastructure, must be installed within 30 days of release. See the manager, Corporate Information Security Office (CISO), to request access to a specific Postal Service configuration hardening standard.

Secure System Configuration: Software developers and COTS software suppliers must provide secure configuration guidelines that fully describe all security relevant configuration options and their implications for the overall security of the software and system.

a. The guideline shall include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security.

b. Developers must determine how to configure each setting that has an effect on security so the default configuration settings are secure and they do not weaken the security functions provided by the platform, network infrastructure, or services.

8-2.4.3 Change and Version Control

Changes to information resources and configurations must be managed to ensure that Postal Service information resources are not inadvertently exposed to unnecessary risks and vulnerabilities and that only qualified and authorized individuals initiate changes, upgrades, and modifications. Individual access privileges must be approved by appropriate management officials.

All changes must be appropriately approved and documented. Application code changes are managed using version control software. Change control records must be maintained to support and document system software maintenance, software and hardware upgrades, and any local system modifications.

8-2.4.4 Patch Management

An effective patch management process must be implemented to investigate, prioritize, test, track, control the deployment and maintenance of software releases, and resolve known security vulnerabilities. The patch management process must address all information resources installed in the Postal Service computing environment. Security patches must be installed in accordance with the agreed upon schedule and following established evaluation and implementation processes. Critical security patches for PCI- related information resources, including applications and infrastructure, must be installed within 30 days of release. Software security patches must be evaluated on a regular basis. The evaluation period varies by platform and is defined in the applicable hardening standard. If the patch is appropriate for the Postal Service environment, the patch must be tested and approved by Postal Service management prior to implementation. Software patch

evaluations and testing must be properly documented and retained in the appropriate repository that is available for audit purposes. Personnel involved in the patch management process must be appropriately trained to ensure a viable vulnerability remediation process.

Patch management involves acquiring, testing, and installing multiple patches (code changes) to software systems, including operating system software, supporting software and packages, firmware, and application software. Patch management tasks include the following:

a. Maintaining current knowledge of available patches.
b. Deciding what patches are appropriate for particular information resources.
c. Prioritizing the patches to be installed.
d. Testing patches in a nonproduction environment first in order to check for unwanted or unforeseen side effects.
e. Developing a back-out plan which includes backing up the systems about to be patched to be sure that it is possible to return to a working configuration.
f. Securing management approval.
g. Ensuring that patches are installed properly.
h. Testing information resources after installation.
i. Documenting all associated procedures, such as specific configurations required.

Patch management is critical to ensure the integrity and reliability of information resources. Patch management should be capable of:

a. Highly granular patch update and installation administration (i.e., treating patches and mainframes, servers, desktops, and laptops separately).
b. Tracking machines, and updating and enforcing patches centrally.
c. Verifying successful deployment on each machine.
d. Deploying client settings, service packs, patches, hot fixes, and similar items network-wide in a timely manner in order to address immediate threats. Critical security patches for PCI-related information resources, including applications and infrastructure, must be installed within 30 days of release.
e. Initiating from a central management console.
f. Providing scheduling, desktop management, and standardization tools to reduce the costs associated with distribution and management.

g. Providing ongoing deployment for both new and legacy systems in mixed hardware and operating system environments.

h. Automating the repetitive activity associated with rolling out patches.

i. Analyzing the operating system and applications to identify possible security holes.

j. Scanning the entire network (IP address by IP address) and providing information such as service pack level of the machine, missing security patches, key registry entries, weak passwords, users and groups, and more. For MPE and MHE systems, a scan schedule must be reviewed with system owners to prevent needless negative impact to mail processing and logistics operations.

k. Analyzing scan results using filters and reports to proactively secure information resources (e.g., installing service packs and hotfixes).

8-2.4.5 Security Testing of the Configuration

After the information system is changed, the security controls must be checked to ensure the security features are still functioning properly. Periodically (at a minimum annually), the security controls must be tested to ensure the information security controls are functioning as designed and documented.

Significant changes will cause the re-initiation of the C&A process. The criteria for initiating a recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process*, 6-2.

8-2.5 Separation of Duties

An individual or organization must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for accidental or malicious wrongdoing, fraud, or collusion. When it is not possible for duties to be assigned to separate individuals, the roles and functions performed must be clearly defined, associated activities logged, security-related functions audited, and compensating controls identified and implemented. The CISO reserves the right to validate the effectiveness of the compensating controls.

8-2.6 Application Source Code

Application source code is considered business proprietary information by the Postal Service and is expected to be handled and stored in a secure manner. When source code is consolidated and stored in a repository/vault, that repository/vault is considered sensitive and must adhere to the following controls:

a. The repository/vault must be in a controlled area and physical access to the repository/vault will be controlled through an access control system.

b. Electronic access to the repository/vault will be controlled through eAccess/ARIS.

c. A fully accountable check-in/check-out process must be operational.

d. Code may not be removed from the vault without using the approved check-in/check-out process.

e. Any code that is removed from the vault must be protected from unauthorized access or usage.

f. Business partners having access to code must have a valid Postal Service nondisclosure agreement (NDA) on file with the Postal Service. Business partner NDAs will be filed with the contracting officer.

g. A defined process of separation of duties must be implemented to support code propagation through the environments (e.g. developers will not have the ability to place code directly into the production environment).

h. A versioning system must be in-place to ensure that proper version control is maintained.

8-2.7 Developers

A developer is an employee or contractor with the development-related responsibilities (e.g., the ability to check-in code or make changes to source code, scripts, or configuration files) and as such must be included in the Postal Service Corporate Developer Registry (CDR).

The following restrictions apply to all developers:

a. Developers are not authorized to be production application/platform administrators.

b. Developers are not authorized to copy production data.

c. Developers are not authorized to have greater than read access to the underlying operating system.

d. Developers are not authorized to have greater than read access to the underlying database.

e. Developers are not authorized to have greater than read access to the application (i.e., under no circumstances are developers ever allowed to have privileged or administrative access to the application).

f. Developers are not authorized to promote code to the production environment.

g. The definition of developer is global in scope, and these restrictions apply across all applications and platforms.

8-2.8 Application Security

To address today's threat environment, developers must employ some of the new application controls that are harder to evade and more effective than many of the traditional security controls currently employed.

8-3 Operations Security

8-3.1 Distributed Postal Computing Environment

The TSLC defines the following four logical distributed postal computing environments (PCE) as follows:

a. Development (DEV). DEV includes subcategories Sandbox and Inactive.

b. System Integration Testing (SIT).

c. Customer Acceptance Testing (CAT). CAT includes subcategories Training, Quality Assurance (QA), and Pre-Production (Pre-Prod).

d. Production (PROD). PROD includes subcategories Pilot, Certification, Testing Environment for Mailers (TEM), and Disaster Recovery (DR).

The use of any other PCE name or subcategory is not authorized. National systems/applications must be engineered with a minimum of three separate environments with appropriate separations of duties. The three separate environments must have at least four logical environments that are DEV, SIT, CAT, and PROD. In a three-separate environment approach, the acceptable groupings of these four logical environments in the three separate environments are DEV/SIT, CAT, PROD or DEV, SIT/CAT, PROD. In the latter grouping, the SIT environment must be cleared before it becomes the CAT environment.

8-3.2 Environment Restrictions

Restrictions are defined for the following distributed PCEs including the subcategories noted above:

a. DEV.

b. SIT.

c. CAT.

d. PROD.

Separation of duties and other restrictions defined for each of the PCEs must be maintained. Modification of environment restrictions is not authorized.

8-3.2.1 Development Environment

Developers get full access (e.g., read, write, execute, allocate, and delete) in this environment to application software. Restrictions for the development environment include the following:

a. Developers are restricted to read and execute privileges for database and operating system software.

b. Personally identifiable information (PII), which is defined in 3-2.4.2, and payment card industry (PCI) primary account number (PAN) must not be used in this environment.

c. No access to production systems is allowed from this environment.

d. Development environment is an isolated infrastructure (DEVSUB) or enclaved.

e. Use of non-sensitive production information in this environment requires the creation of a generic production data usage letter (PDUL). This letter approves the use of non-sensitive production data until the end of the current fiscal year. The PDUL is needed only for the application to be tested not for every system the application touches.

f. Use of sensitive or sensitive-enhanced production information in this environment requires:

(1) A specific PDUL that approves the use of this data for (1) one year from the time of the request, at which time another PDUL will be required. The PDUL is needed only for the application to be tested, not for every system the application touches.

(2) The development environment must implement the same controls as the production environment or the PII or PCI PANs, and sensitive information must be de-identified in the production environment before data is transferred to the development environment. The project manager must validate (and attest in a letter to the CISO and the privacy office) that all PII and PCI PANs, and sensitive information have been de-identified.

g. All connections of developer workstations to databases in all environments must be added as a temporary request for no more than 6 months with the option to renew when the NCRB team (coordinating with the ISSO) contacts the requester prior to expiration; contact the users

listed in the database connections in the general tab of ServiceNow. This fits the 6-month access review policy.

h. All connections for developers will be from their workstations/laptops and not from a subnet.

8-3.2.2 **SIT Environment**

Developers have full access (e.g., read, write, execute, allocate, and delete) in this environment to application software. Code is migrated from the SIT environment back to the development environment to apply updates/fixes. Restrictions for the SIT environment include the following:

a. Developers may have access to the SIT environment with documented management approval.

b. Systems moved to the SIT environment are documented and managed by a version control library system.

c. PII and PCI PANs and sensitive information must not be used in this environment.

d. Use of non-sensitive production information in this environment requires a generic PDUL that approves upfront the use of non-sensitive production data for up to 1 year from the time of the request until the application requires recertification and reaccreditation at which time another PDUL will be required.

e. Use of production PII and PCI PANs, and sensitive information in this environment requires:

(1) A specific PDUL that approves the use of this data for 1 year from the time of the request; then they would be required to request another PDUL. The PDUL is only needed for the application to be tested not for every system the application touches.

(2) The SIT environment must implement the same controls as the production environment or the PII, or PCI PANs, and sensitive information must be de-identified in the production environment before the data is transferred to the SIT environment. The project manager must validate (and attest in a letter to the CISO and the privacy office) that all PII, and PCI PANs, and sensitive information have been de-identified.

f. All connection of developer workstations to databases in all environments must be added as a temporary request for no more than 6 months with the option to renew when the NCRB team (coordinating with the ISSO) contacts the requester prior to expiration; contact the users listed in the database connections in the general tab of

ServiceNow. This fits the 6-month access review policy.

g. All connections for developers are from their workstations/laptops and not from a subnet.

8-3.2.3 CAT Environment

Access is restricted to production operations personnel, executive sponsorship, and developers with proper authorization. The CAT environment must implement the same controls and security requirements as production. Restrictions for the CAT environment include the following:

a. Developers may have access to the CAT environment with documented management approval.
b. Systems moved to the CAT environment are documented and managed by a version control library system.
c. PCI PANs must not be used in this environment.

d. PII and sensitive information must be de-identified prior to use in the CAT environment; any exceptions to the de-identification requirement must be approved by the CIO, CPO, and the executive sponsor. If PII that is not de-identified is approved for use in the CAT environment, the PII and sensitive information must be encrypted.
e. Use of non-sensitive production information in this environment requires a generic PDUL that approves upfront the use of non-sensitive production data for up to 1 year from the time of the request until the application requires recertification and reaccreditation at which time another generic PDUL is required. See 8-3.2.5, Other Environments.
f. Use of PII, and PCI PANs, sensitive information in this environment requires:

(1) A specific PDUL that approves the use of this data for (1) one year from the time of the request, at which time another PDUL is required. The PDUL is only needed for the application to be tested, not for every system the application touches.

(2) The CAT environment must implement the same controls as the production environment or the PII and PCI PANs, and sensitive information must be de-identified in the production environment before data is transferred to the CAT environment. The project manager must validate and attest in a letter to the CISO and the Privacy Office that all PII and PCI PANs, and sensitive information have been de-identified.

(3) All connection of developer workstations to databases in all environments must be added as a temporary request for no more than 6 months with the option to renew when the NCRB team (coordinating with the ISSO) contacts the requester prior to expiration; contact the users listed in the database connections in the general tab of ServiceNow. This fits the 6-month access review policy.

(4) All connections for developers will be from their workstations/laptops and not from a subnet.

8-3.2.4 Production Environment

Restrictions for the production environment include:

a. Developers must not have ongoing read access or privileged access to application, database, and operating system software in this environment.

b. Developer access to production systems must be authorized by the executive sponsor, CIO or designee, and CPO via eAccess/ARIS or PS Form 1357, *Request for Computer Access.* PS Form 1357 is only to be used for applications where eAccess/ARIS is unable to handle the requested computer access.

c. Developer access to the production system, if approved in eAccess/ARIS, must be managed and documented in eAccess/ARIS.

d. A Remedy Problem Ticket must be opened to implement the approved access to the production system and the access must be removed when the Problem Ticket is closed.

e. The developer account must be temporary and disabled/removed upon completion of the task.

f. Developer access must be logged while the account is active.

g. The CISO must be informed of the access.

h. Production data must not be copied by the developer.

i. Extreme care must be exercised when accessing PII and cardholder information. If not necessary for the task, PII and cardholder data must be masked from view or de-identified. Masking is the method of concealing portions of cardholder data when displayed or printed. De-identifying production data is the process of systematically transforming PII and cardholder data elements so they can no longer be used identify an individual or cardholder data. When masking the PAN, the first six and the last four digits are the maximum number of digits to be displayed or printed.

j. Sensitive and sensitive-enhanced information must be protected according to the requirements in 3-5.

8-3.2.5 Other Environments

The restrictions are the same as for the development environment.

8-3.3 Testing Restrictions

All information resources must comply with the testing restriction policies below.

The SIT and CAT environments must be representative of the operating landscape, including likely workload stress, operating system, application software, database management systems, and network/computing infrastructure found in the production environment. As the production environment changes, the test environment must also change to stay in synchronization.

The testing must only be conducted within the CAT environment by a test group independent from the development team using clearly defined test instructions (scripts) and interactive testing that adequately address the testing requirements and success criteria defined in the test plan. Errors found during testing must be logged, classified (e.g., minor, significant, and mission critical), and communicated to key stakeholders.

8-3.3.1 Development and Testing in the Production Environment

Development and testing of hardware and software must not be performed in the production environment. Engineering development and testing are in the production environment except as planned and implemented by MPE/MHE.

8-3.3.2 Testing With Non-sensitive Production Data

Prior approval in writing is required from the executive sponsor and CIO or designee if non-sensitive production data is to be used in a test environment, regardless of where the testing is conducted. Such approved production data files must be identified as "copies" to prevent them from being reentered into the production environment.

8-3.3.3 Testing with Sensitive-Enhanced and Sensitive Production Data

Prior approval in writing is required from the CPO, executive sponsor, and CIO or designee if sensitive-enhanced and sensitive information is to be used in a test environment, regardless of where the testing is conducted. Approved data files must be identified as "copies" to prevent them from being re-entered into the production environment.

Prior to usage of production data in a test environment, the test environment must be hardened to production standards.

PII or cardholder data must not be placed in the test environment without being de-identified. The masked/transformed data elements must then be propagated across related tables within the database to preserve the integrity of data relationships, maintain the referential integrity of the test data, and ensure the validity of test results.

8-3.3.4 Testing at Non-Postal Service Facilities with Production Data

Additional approval in writing is required from the manager, CISO, if production data is to be used in a test environment outside of Postal Service facilities. Such approved files must be identified as "copies" to prevent them from being re-entered into the production environment.

8-3.4 Compensating Controls in lieu of Production Data Usage Letters

The following compensating controls must implemented in lieu of Production Data Usage Letters (PDULs):

a. Current eAccess/ARIS approvals for accessing production data in a nonproduction environment.

b. Information resource used to access this data must have a content management solution deployed that restricts the removal of PII and PCI cardholder information from the information resource.

c. Information resource used to access this data must have an encryption solution that meets Postal Service standards.

d. Users must shut down the information resource before leaving for the day.

e. Data masking must be implemented, where feasible, on development and test servers to protect PII and PCI cardholder information. Masking must be performed in a manner that does not expose the original file to unauthorized access and must be appropriately destroyed after the masked data version is created.

f. If data is transferred to an end point information resource, the transport method must employ an encryption solution that meets Postal Service standards.

g. Users must be on Postal Service premises for these compensating controls to be applicable; these compensating controls are not sufficient for remote off-site access.

h. Information resources engaged in accessing production data in a nonproduction environment are subject to 'data at rest' scans.

8-4 Certification and Accreditation

C&A is a formal security analysis and management approval process to assess residual risk before the resource is put into production. Each phase of the TSLC has corresponding security activities that must be performed to maintain a secure environment and comply with Postal Service policies and legal requirements. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for more details.)

8-4.1 What the C&A Process Covers

The C&A process consists of (9) nine interrelated phases that are conducted concurrently with the development and deployment of new information resources. The objectives of the C&A are to assess threats, define security requirements and controls, test security solutions, and evaluate the security controls and processes chosen to protect the information resource.

Sensitive-enhanced, sensitive, critical-high, and critical-moderate information resources must complete the C&A process culminating with the certification ad accreditation of the information resource. Both approvals (i.e., certification and accreditation) are required before beginning operations.

All wireless information resources, regardless of sensitivity or criticality, must complete the C&A process.

8-4.2 When C&A Is Required

The C&A is required for the following:

a. All information resources, regardless of whether they are located at a Postal Service or non-Postal Service facility or whether they are controlled directly by the postal Service or through a contractor or business partner.

b. All wireless information resources, regardless of sensitivity or criticality, must complete the C&A process.

c. Pilot projects or proof of concept for information systems prior to processing production or live data.

The frequency for recertification and reaccreditation is defined in the Re-Initiate C&A section. Refer to section 8-5.8.8 Reinitiate C&A

Interim Authority To Test

An IATT is a temporary authorization to test an information resource within any owned or operated Postal Service information environment. The information environment of interest will process, store, or collect Postal Service data under a short time frame per a predetermined set of conditions or constraints. An IATT may also be used to field new systems or capabilities for a limited time (such as Proof of Concept), with a limited number of platforms to support developmental efforts, demonstrations, or exercise.

*Note: An IATT is **only** required if an information resource meets the conditions explained above. An IATT is not required for every information resource.*

IATTs are granted for a limited duration of either 30, 60, or 90 days with an option for one extension. The IATT process may not be used to avoid authorization or validation activity and certification determination requirements for authorizing a system to operate.

It is Postal Service policy that all information systems, applications and services (referred to collectively as (information system (IS)) will be certified through the appropriate Postal processes as identified in Handbook AS- 805-A. All uncertified ISs that are to be fielded for a limited time (such as a Proof of Concept), with a limited number of platforms to support developmental efforts, demonstrations, or exercise shall

receive an IATT prior to connecting to a live (production) network. ISs receiving an IATT will not be used for operational activities; the IATT is granted for testing purposes and to support demonstrations and exercises. This testing may include limited user testing, independent validation and verification testing to facilitate Postal Service certification.

8-4.3 Value of C&A Process to the Postal Service

C&A demonstrates that the Postal Service has taken due care to protect its information resources in accordance with policies and legal requirements defined by its business, legal, and administrative entities and ensures that the security measures implemented to protect such resources are documented.

8-4.4 Access to Information Resources and Related Documentation

During the C&A process, the manager, CISO, or designated agent has unrestricted access to the information resources and related documentation.

8-4.5 Independent Processes

Independent processes are evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information resources. The following independent processes may be conducted by an organization that is separate and distinct from those responsible for the development and operation of the information resource and that strictly adheres to the separation-of-duties policy:

a. Independent risk assessment.

b. Independent security code review.

c. Independent penetration testing and vulnerability scans.

d. Independent security test validation.

Additional information is available in Handbook AS-805-A, *Information Resource Certification and Accreditation Process.*

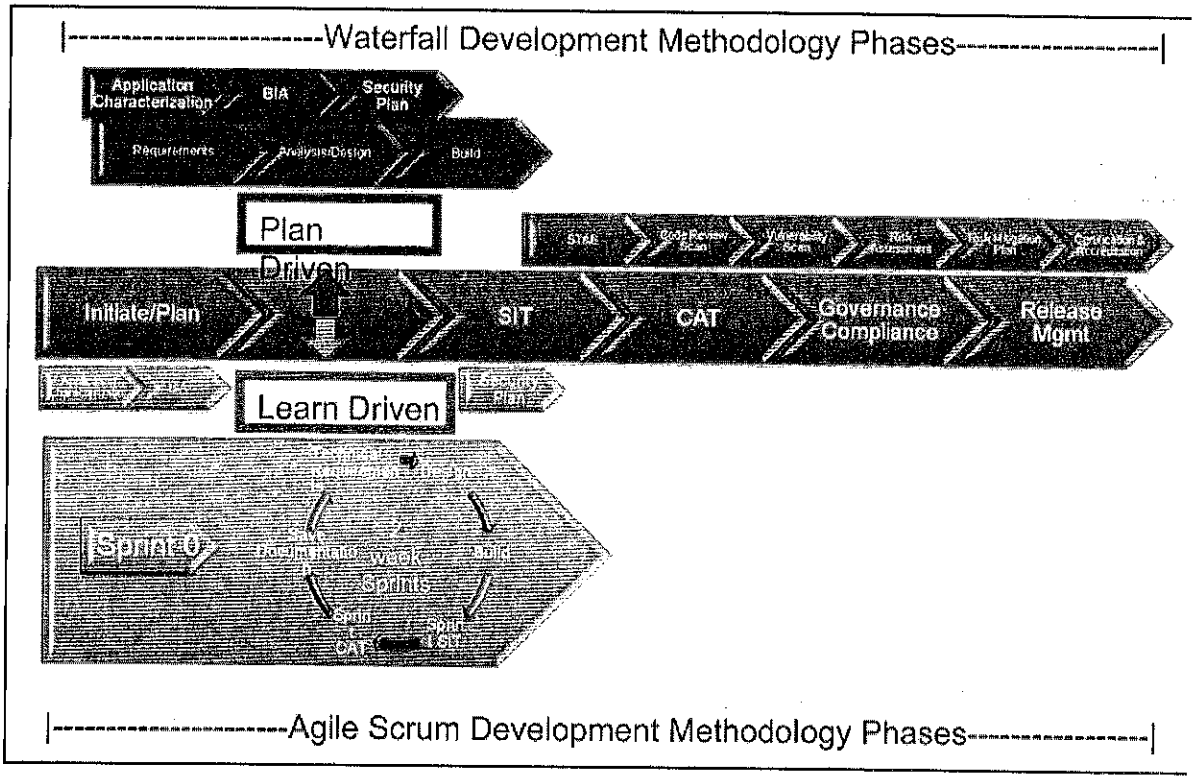
8-4.6 Contractual Terms and Conditions

Contract language and partnering agreements must reflect the information security requirements of the Postal Service defined in the C&A process. The executive sponsor is responsible for ensuring that the security requirements are included in all contracts that involve developing information resources and all contracts with businesses that transmit information to or from trusted Postal Service networks.

8-5 Information Resource C&A

Exhibit 8-5 depicts the seven phases of the Waterfall and Agile Scrum Development Methodologies and the major documents (deliverables) for each phase. The information security activities associated with the C&A phases are described in the following paragraphs.

Exhibit 8-5
Seven C&A Phases



8-5.1 Phase 1 — Initiate and Plan

Phase 1 determines what will be required during the C&A and the magnitude of the effort needed to complete the C&A process. The process is initiated for all information resources regardless of their location or whether they are controlled directly by the Postal Service or through a contractor or business partner. Information resources may be referred to as a technical solution within the TSLC. The C&A process can be applied to pilot, new, and production applications, infrastructure, and business partner initiatives.

8-5.2 Phase 2 — Requirements

Phase 2 determines the information security requirements and begins to assess the risks. The information security

activities of Phase 2 are described in the following paragraphs.

8-5.2.1 Conduct Business Impact Assessment

An Impact Assessment is completed to determine the level of sensitivity and criticality and the information security requirements for the information resource.

8-5.2.1.1 Determine Sensitivity and Criticality

The Privacy Impact Assessment is completed followed by the determination of sensitivity and criticality for all information resources.

8-5.2.1.2 Determine Security Requirements

Security requirements are defined for all information resources to secure the information resources commensurate with the risk. Security requirements include the following:

a. Baseline security requirements for all information resources.

b. Additional security requirements based upon the sensitivity and criticality of the information resource, legislation, regulations, directives, and industry requirements.

c. Additional conditional requirements based on request by senior management or specific criteria.

d. Additional security requirements recommended by the information system security officer (ISSO) based on generally accepted industry practices, the operating environment, and the risks associated with the information resource.

8-5.3 Phase 3 — Design

Based on the security requirements defined in the BIA, the security controls and processes for the information resource are defined. The information security activities of Phase 3 are described in the following paragraphs.

8-5.3.1 Develop High-Level Architecture

A high-level architectural diagram is developed and maintained current for all information resources documenting hardware, communication services and ports used, security devices, and interconnected resources. The architectural diagram is used by the manager, CISO ISS to determine the impact on the infrastructure and the need for additional security controls such as an enclave (see 11-3.7, Determining When a Secure Enclave Is Required).

8-5.3.2 Identify Internal and External Dependencies

Internal and external dependencies must be identified and documented in the eC&A process.

8-5.3.3 Document Security Specifications

If information resource is contracted, security specifications are documented to satisfy the security requirements defined by the BIA.

8-5.3.4 Select and Design Security Controls

Identify potential security controls (safeguards) based on the information security requirements and in light of business requirements including project schedule and budget.

An analysis of potential controls is conducted to determine their potential effectiveness to remove, transfer, or otherwise mitigate risk to information resources. The controls analysis identifies any residual risk to the information resource.

A cost-benefit analysis is performed and documented to facilitate the implementation of cost-effective protection for information resources.

Safeguards are selected or designed based on the controls analysis and the cost-benefit analysis.

8-5.3.5 Develop Security Plan

A security plan must be developed for all information resources. A security plan is a blueprint for designing, building, and maintaining an information resource that can be defended against threats, including intruders, both internal and external. The security plan covers both the nonproduction and production environments and describes all information security controls that have been implemented or planned.

8-5.3.6 Conduct a Site Security Review

The site security review assesses the physical security controls of facilities hosting sensitive-enhanced, sensitive, and critical information resources. The lack of adequate physical security controls could affect the availability, confidentiality, and integrity of Postal Service applications and the information resources hosting them. A site security review may not be required if the site is accredited by a government agency.

Site security reviews of non-Postal sites storing PCI cardholder information must be conducted annually but should be conducted more frequently if it is deemed there is increased risk.

The site security review results in a report and not a Postal Service certification or accreditation.

8-5.4 Phase 4 — Build

The security controls and processes selected and defined in Phase 3 for the information resources are implemented in this Phase. The information security activities of Phase 4 are described below.

8-5.4.1 Develop, Acquire, and Integrate Security Controls

Appropriate security controls are developed in house, acquired, or outsourced depending on the cost-benefit analysis and integrated into the information resources and related processes.

8-5.4.2 Hardening Information Resources

Information resources hosting sensitive-enhanced, sensitive, and critical applications and information resources that are part of the Postal Service infrastructure must be hardened to meet or exceed the requirements documented in Postal Service hardening standards. Hardening refers to the process of implementing additional software, hardware, or physical security controls. Hardening standards are based off of Center of Internet Security (CIS) sources, vendor recommended setting and industry best practices. If a benchmark is not developed by CIS sources, vendor recommended security settings are established by the Postal Service.

8-5.4. Develop Security Operating Procedures

Security operating procedures for emergencies, separation of duties, secure computer operations, manual processes, etc., must be developed for all information resources.

8-5.4. Develop Operational Security Training

Appropriate materials are developed for training users, system administrators, managers, and other personnel on the correct use of the information resource and its security controls.

8-5.4.5 Incorporate Security Requirements in Service Level agreements and Trading Partner Agreements

Service level agreements (SLAs) may be developed for in-house managed and/or developed information resources. Trading partner agreements (TPAs) are often developed for externally managed and/or developed information resources. If SLAs or TPAs are developed, incorporate information security requirements. Information security requirements for securing cardholder data must be incorporated in contracts and memoranda of understanding (MOU) with PCI service providers.

MOUs document the terms and conditions for interagency data and information sharing in a secure manner. An interconnection security agreement (ISA) supports the MOU by specifying the requirements for connecting IT systems and describing the security controls that will be used to protect the systems and data via the certification and accreditation (C&A) process.

8-5.4.6 Register Information Resource in eAccess/ARIS

Register the information resource in eAccess/ARIS, which is the Postal Service application for managing the authorization process for personnel needing to access the information resource and the associated information. Registration is also required for the use of managed accounts (e.g., machine accounts).

8-5.4.7 Develop Business Continuity and Facility Plans

Business continuity plans must be developed for critical information resources. A facility recovery plan is developed for facilities designated by the vice president Information Technology Operations as major information technology sites. These plans are started during this phase and updated in Phase 5 – System Integration Testing.

8-5.4.8 Identify Connectivity Requirements

Requirements for connectivity to the Postal Service infrastructure must be identified and a request must be submitted to the Network Change Review Board (NCRB) *(see https://usps.service-now.com).*

8-5.5 Phase 5 — System Integration Testing

The security controls and processes implemented in Phase 4 are tested. The information security activities of Phase 5 are described in the following paragraphs.

8-5.5.1 Develop Security Test Plan

A security test plan must be developed for all information resources. The security test plan evaluates the technical and nontechnical security controls and other safeguards to establish the extent to which the information resource meets the security requirements for its mission and operational environment.

8-5.5.2 Conduct Operational Security Training

Using the training materials developed in the prior phase, users, system administrators, managers, and other personnel are trained on the correct use of the information resource and its security safeguards.

8-5.5.3 Conduct Development of Contingency Plans

The contingency plans (and, if applicable, the facility recovery plan) from Phase 4 – Build must be updated as required.

8-5.6 Phase 6 — Customer Acceptance Testing

Phase 6 consists of activities described below that culminate in the certification, risk mitigation plan, accreditation, acceptance of residual risk, and approval to deploy an information resource. (See Handbook AS-805-A Exhibit 4-6 for The Certification and Accreditation Input, Activities and Output.)

8-5.6.1 Conduct Security Test and Document Results

Security testing is conducted using the approved security test plan. If a modification to a control is required, the change

must be reflected in the security plan and the security test plan before the test is executed. The results of the testing must be documented and communicated in language that is understandable to business-process owners and the ISSO.

(See Handbook AS-805-A Section 4-6.4.2.1 for Conduct The Security Test and Evaluation.)

8-5.6.2 Conduct Security Code Review

To protect the infrastructure, a documented security code review may be required. (See Handbook AS-805-A for the criteria for conducting a code review.)

The security code review is based on the Postal Service Security Code Review Standards or an acceptable equivalent. This security code review is not required if an independent security code review is conducted.

8-5.6.3 Conduct Vulnerability Scan

A vulnerability scan is recommended for all information resources. A quarterly vulnerability scan is required for PCI applications and an annual vulnerability scan is required for externally facing applications. The scanning procedure must ensure adequate scan coverage and the updating of a list of vulnerabilities.

8-5.6. Conduct Risk Assessment

A risk assessment must be conducted for all information resources to identify security concerns (e.g., threats, vulnerabilities, and control weaknesses), risk ranking, additional countermeasures, and residual risk (see 4-3, Information Resource Risk Management). The risk assessment can be started in this phase but must be updated throughout the TSLC.

8-5.6.5 Conduct Independent Risk Assessment

An independent information security risk assessment may be required to evaluate the appropriateness and effectiveness of the security controls and identify residual risk. (See Handbook AS-805-A for the criteria for conducting an independent risk assessment.)

8-5.6.6 Conduct Independent Security Code Review

Information resources may be subject to an independent code review of the source code and documentation to verify compliance with software design documentation and programming standards and the absence of malicious code. The independent code review may also evaluate correctness and specific security issues. (See Handbook AS-805-A for the criteria for conducting an independent security code review.)

8-5.6.7 Conduct Independent Penetration Testing and Vulnerability Scans

Independent penetration testing evaluates the effectiveness of the implemented information resource configuration. Vulnerability scans evaluate information resources for vulnerabilities and compliance with Postal Service

information security policies and standards. (See Handbook AS-805-A for the criteria for conducting independent penetration testing and vulnerability scans.)

8-5.6.8 Conduct Regular Vulnerability Scans

Vulnerability scans evaluate information resources for vulnerabilities and compliance with Postal Service information security policies and standards. (See Handbook AS-805-A for the criteria for conducting independent penetration testing and vulnerability scans.)

8-5.6.9 Perform Penetration Testing

Prior to the first production deployment, or "go live" date, all Postal applications should have penetration testing performed. Operational requirements for penetration testing include ensuring that the system is available for testing, and that penetration testers have access to the application and data nearly identical to a live environment. Objectively, penetration testing should ensure that the application is free of any findings prior to any customer interaction with the application. Postal leaders are responsible for ensuring that enough time is available for the application to be tested.

8-5.6.10 Conduct Independent Validation of Security Testing

The independent security test validation addresses the appropriateness and effectiveness of the security controls and corroborates the previously conducted security test results. The scope of the independent security test validation depends on the information resource, its environment, and the associated threats and vulnerabilities. The independent security test validation is usually carried out at the development or test site. (See Handbook AS-805-A for the criteria for conducting an independent security test validation.)

8-5.6.11 Project Manager and ISSO Develop C&A Documentation Package

Sensitive-enhanced, sensitive, and critical information resources require a C&A documentation package. The project manager and the ISSO develop the C&A package. The package is a consolidation of the designation of sensitivity and criticality and associated protection requirements (BIA); threats, vulnerabilities, additional controls, and residual risks (risk assessment); protection mechanisms (security plan and business continuity plans); and the security test and evaluation results.

8-5.6.12 Project Manager, Executive Sponsor, and ISSO Prepare Risk Mitigation Plan

The Project Manager, Executive Sponsor, and ISSO prepare a risk mitigation plan for any residual risks rated as medium or high, recommending how the risks will be mitigated, the organization or individual responsible, and the time table for resolution.

8-5.6.13 ISSO Reviews C&A Documentation Package and Prepares Evaluation Report

The ISSO reviews the C&A documentation package and prepares a C&A evaluation report highlighting the findings and recommendations. The ISSO escalates security concerns or forwards the C&A evaluation report and supporting documentation to the certifier for review.

8-5.6.14 Certifier Escalates Security Concerns or Certifies Information Resource

The certifier (e.g., manager, C&A process) reviews the C&A evaluation report and the supporting C&A documentation package, escalates security concerns or prepares and signs a certification letter, and forwards the certification letter and C&A documentation package to the accreditor.

If the certifier decides not to certify the information resource, he or she will indicate the C&A Phase to return to for rework.

8-5.6.15 Accreditor Escalates Security Concerns or Accredits Information Resource

The accreditor (i.e., manager, CISO) reviews the risk mitigation plan and the supporting C&A documentation. Based on this review, the accreditor either, escalates security concerns or prepares and signs an accreditation letter, and forwards the accreditation letter and final C&A documentation package to the vice president functional business area (or the executive sponsor if this responsibility is delegated) and to the vice president of IT (or the Business Relationship Management portfolio manager if this responsibility is delegated).

If the accreditor decides not to accredit the information resource, he or she will indicate the C&A phase to return to for rework.

8-5.7 Phase 7 – Governance and Compliance

No information security activities are associated with this phase.

8-5.8 Phase 8 — Release Management and Production

Phase 7 is the operation and maintenance period of the information resource and includes activities to ensure that chosen security controls and procedures are functioning properly and that security controls are modified or added as needed to continue to protect the information resource. The information security activities for Phase 7 are described in the following paragraphs.

8-5.8.1 Data Conversion

A data conversion plan must be defined so that it incorporates collecting, converting, and verifying data for completeness and integrity and resolving any errors found during conversion. Create a backup of all data prior to

conversion and maintain audit trails to track the conversion to ensure there is a fallback and recovery plan in case the conversion fails. Ensure that the backed-up data conforms to the applicable data retention schedule.

8-5.8.2 Deploy Information Resource

Certification and accreditation approvals are both required before deploying the information resource. When the information resource is deployed, the security controls for the information resource are implemented as documented in the security plan and with the caveats included in the acceptance letter.

8-5.8.3 Information Resource Maintenance

Information resources must be maintained in a timely manner. Critical security patches for PCI-related information resources, including applications and infrastructure, must be installed within 30 days of release. The tools, techniques, and mechanisms used to maintain information resources must be properly controlled.

8-5.8.4 Follow Security-Related Plans and Continually Monitor Operations

The security-related plans must be followed during deployment, operation, and maintenance. The information resource controls must be continually monitored by the project team to ensure they are working as intended and remain in compliance with the security-related plans.

8-5.8.5 Periodically Review, Test, and Audit

Information resources are periodically reviewed, tested, and audited for compliance with Postal Service policies (e.g., plans related to facility recovery or business continuity are tested to ensure that these plans meet business and security objectives).

For non-PCI information resources, a subset of the information security controls must be formally tested annually by the project team, the tests documented, and the results submitted to the applicable ISSO. The security controls that are volatile or critical to protecting the information system must be assessed at least annually. All other controls must be assessed at least once during the information resource's 3-year accreditation cycle (e.g., one third of these other controls each year).

8-5.8.6 Reassess Risks and Upgrade Security Controls

Risks are re-assessed as part of the re-initiation of the C&A process. Security controls are upgraded as necessary to protect the information resource and assure business continuity.

8-5.8.7 Update Security-Related Plans

Security-related plans are updated in response to changing environment, changing technology, re-assessed risks or

vulnerabilities, and as part of the re-initiation of the C&A process.

8-5.8.8 Reinitiate C&A

The criteria for recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process.*

8-5.8.9 Disposition C&A Documentation

After each information resource has been accredited, zip the electronic versions (PDFs) of the C&A documents and store them in the IT TSLC Artifacts Library for access by the project manager and their project development team. Keep the electronic C&A documents for 4 years after the information resource is accredited.

Keep the hardcopy documents for 1 year after the information resource has been accredited and then destroy in accordance with 3-5.8.

8-5.9 Phase 9 - Retire

8-5.9.1 Dispose of Data

All Postal Service sensitive-enhanced, sensitive, and critical information that is no longer needed, whether in electronic or nonelectronic format, is transferred, archived, or destroyed in accordance with official Postal Service policies and procedures (see 3-5.8, Disposal and Destruction of Information and Media, and Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management).*

8-5.9.2 Sanitize Equipment and Media

All Postal Service sensitive-enhanced, sensitive, and critical information is completely erased or destroyed prior to disposal of the hardware or electronic media on which it resides (see 3-5.8, Disposal and Destruction of Information and Media).

9 Information Security Services

9-1 Policy

Information security services provide the policies, requirements, standards, and processes that enable the integration and implementation of information security across Postal Service information resources to ensure a viable secure computing infrastructure and to protect information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction.

All Postal Service personnel must adhere to the following information security services:

a. Authorization.

b. Accountability.

c. Identification.

d. Authentication.

e. Confidentiality.

f. Integrity.

g. Availability.

h. Security administration.

i. Audit logging.

9-2 Security Services Overview

Information security services provide the framework for implementing information security measures used to protect information resources. Security services are as follows:

a. Authorization determines whether, and to what extent, personnel should have access to specific computer resources.

b. Accountability associates each unique identifier with one user or system process to enable tracking of all actions by the user or of the process on the information resource.

c. Identification associates a user with a unique identifier (i.e., user account or log-on ID) by which that user is held accountable for the actions and events initiated by the identifier.

d. Authentication verifies the claimed identify of an individual, computing device, or originator.

e. Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

f. Integrity ensures the correct operation of information resources, consistency of data structures, and accuracy of stored information.

g. Availability ensures information resources are accessible by authorized personnel or other information resources when required.

h. Security administration implements management constraints, operational procedures, and supplemental controls established to provide adequate protection of an information resource.

i. Audit logging records operational and security-related events.

9-3 Authorization

Authorization provides the framework for determining whether, and to what extent, personnel or on-line users should have access to computer resources. Information resources must be configured to ensure that no user is allowed access to an information resource (e.g., transaction, data, and process) unless authorized by appropriate Postal Service management or approved external user. Upon employment, personnel may be granted access to temporary information services until they receive clearance. External users may need approval to access certain business services. Further details regarding authorization for both internal and external users follow see section 9-3.1

9-3.1 Authorization Principles

Internal Users (workforce):

Access must be granted based on personnel roles and the security principles of clearance, need to know, separation of duties, and least privilege.

External Users (customers):

External User Authorization is the process of giving the user permission to access a specific resource, data set, page/URL or function. Authorization is tied to a business or user service managed by external users. A business or user service translates access authorization to an on-line page/URL, a function, a data set or some other resource. There are a variety of methods used to grant an authorization and a variety of methods used to determine if a user should be authorized to have access to a business service.

a. Methods used to grant an authorization include approval based internal functions and/or external user functions.
b. Internal authorization functions include help desk approval, use of an authorization code (i.e., invitation, promo code or validation code, etc.), identity proofing, credit validation and other Postal Service staff approval methods.

c. External authorization functions include a self-asserted claim by an end user to manage the users associated with a service, a function or function of a company. The first person to make that claim can become the Business Service Administrator (BSA). The BSA then can in turn approve other users to have the same privileges as they do in performing a function or having access to a resource for the same data set. Once a BSA is assigned, external users may then request access to that function or resource. The BSA can either accept the request or deny the request. The BSA can also appoint a delegate who can also make similar approvals. A Delegate approver cannot deny access to a BSA. Some BSA roles are only assigned in coordination with Postal Service personnel to determine the "rightful" owner of that data set or function. Once that BSA is approved by the Postal Service, then the BSA can also add other users to have similar rights.

9-3.1.1 Clearances

For personnel without appropriate clearances or background investigations, access is restricted to temporary information services. Managers must use eAccess/ARIS to request access authorization for individuals who do not have the appropriate clearance and are responsible for the access activities of those individuals.

9-3.1.2 Need to Know

For sensitive-enhanced, sensitive, and critical information resources access must be limited in a manner that is sufficient to support approved business functions. Access to sensitive-enhanced and sensitive Postal Service information resources must be limited to personnel who need to know the information to perform their duties.

9-3.1.3 Separation of Duties

Only authorized personnel are approved for access to Postal Service information resources. This approval must be specific to an individual's roles and responsibilities in the performance of his or her duties and must specify the type of access (e.g., read, write, delete, and execute); specific resources and information; and time periods for which the approval is valid. Separation of duties and responsibilities are considered when defining roles. For special situations where additional control is required, dual authorization can be implemented.

9-3.1.4 Least Privilege

For sensitive-enhanced, sensitive and critical information resources access is based on providing personnel with the minimum level of information resources and system functionality needed to perform their duties. Systems and applications must define as many levels of access as necessary to prevent misuse of system resources and protect the integrity and confidentiality of Postal Service information. Postal Service information resources must be capable of imposing access control based on specific functions (e.g., create, read, update, delete, and execute).

9-3.2 Authorization Management

eAccess/ARIS is the Postal Service application for managing authorization to information resources. eAccess/ARIS centralizes the management of personnel and machine identities (i.e., human and nonhuman accounts/identities) and access rights over the entire life cycle, from account creation/registration to termination. eAccess/ARIS operates on the premise that access is denied unless specifically approved by the user's manager.

External Users (customers) – must receive authorization to the approved application for which access is granted. This includes, but is not limited to, Personal User, Business User, Pending and Partial. For authorization requirements, refer to 9-3.3. For a complete description of account management, refer to 9-4.3 through 9-4.3.4.

9-3.2.1 Requesting Authorization

All requests for authorization to access Postal Service information resources, including temporary information services, must be requested via eAccess/ARIS at *https://eaccess.usps.gov*. If access to a Postal information resource cannot be requested through eAccess/ARIS for any reason associated with a technical limitation of eAccess/ARIS, then use PS Form 1357.

9-3.2.2 Temporary Information Services

Requests for temporary information services must go through eAccess/ARIS for proper management approval. For contractor personnel who have submitted their documentation for security clearances or background investigations, the manager, Corporate Information Security Office (CISO), may authorize temporary access to the following information services until the contractor's background investigation is completed and security clearance has been issued:

a. ACE active directory account.

b. E-mail access.

c. Office suite of services.

d. Intranet browser access.

The following information services are unavailable under temporary access: a.

Internet browser access.

b. Remote access.

c. Access to e-mail except within the Postal Service intranet.

Note: No access beyond temporary information services will be authorized until the background investigation is completed and the appropriate personnel security clearance is granted. Upon receipt of an appropriate security clearance or background investigation, individuals requiring access beyond temporary information services may request additional authorization via eAccess/ARIS.

9-3.2.3 Expiration of Temporary Access Authorization

Temporary access expires in 3 months and can be renewed if warranted.

9-3.2.4 Approving Requests

All requests for authorization must be approved by the individual's manager or supervisor, the contracting officer's representative (if the request is for a contractor), and the executive sponsor of the application.

9-3.2.5 Periodic Review of Access Authorization

Managers must review access granted to personnel under their supervision to ensure that the access is still required for personnel to perform their duties. The minimum acceptable review schedule is on a semiannual basis; more frequent reviews should be scheduled based on information sensitivity.

The manager CISO may require that some privileged system/application accounts be reconciled to related eAccess/ARIS records on a monthly basis. Discrepancies must be investigated and resolved immediately.

9-3.2.6 Implementing Changes

System administrators and database administrators must implement all approved authorization requests for the information resources under their control. They must not add, modify, or revoke access to information resources except in accordance with Postal Service policies.

9-3.2.7 Revoking Access

All managers must ensure that access to information resources is immediately revoked for personnel when no longer required because of a change in job responsibilities, transfer, routine separation or involuntary termination. The immediate manager will advise the system and/or database administrators as to the final disposition of files and data based on the exit date filed by Human Resources.

9-3.2.8 Sudo (Pseudo) Access

Sudo (pseudo) access has higher levels of rights, such as account creation/update/deletion, full application/platform functionality, or a subset of rights that have been designated as privileged. Sudo access must be restricted to a unique individual whose duties require these additional privileges. Use is restricted to performing those job functions required by the privileged access; individuals must use their regular user accounts to perform non-privileged functions. Applications must not have the capability to run as "root." An audit trail must be maintained on all privileged access.

9-3.2.9 User and Resource Registration Management

User and resource registration management must provide the following functionality to allow managers to perform their roles and responsibilities in the authorization process:

a. Register user or resource to directory service or authoritative source.

b. Assign or furnish unique identifier.

c. Track modifications to user or resource access authorizations.

d. Provide management reports.

e. Validate user or resource identity.

f. Revoke or keep user or resource access (two levels of approvals).

g. Log and audit access requests.

9-3.2.10 Special Account Registration Management

Special account (i.e., Service, Shared and Vendor Default) registration management must be implemented to allow managers to identify special accounts under management control and provide appropriate accountability for the account usage from account creation through termination.

Accounts where access is required to perform credentialed scans are often designated within authentication packages such as eAccess/ARIS as "special" accounts. "Special" accounts must not be used for PCI applications unless (a) required by COTS software to function correctly, (b) the account is properly configured (i.e., treated as an administrator account that will not be used as a true service account), and (c) it does not violate other requirements in this handbook.

All special accounts must be documented, registered, and reviewed by responsible managers (i.e., account custodians) monthly. The responsibilities of an account custodian are as follows:

a. Special accounts are assigned to eAccess/ARIS managers who serve as the account custodians.

b. The custodian is ultimately responsible for the use of these accounts with respect to access of Postal Service information systems.

c. Service accounts (e.g., an account managed by Operating System) must be created with the minimum access rights and privileges required to perform the necessary business function and must be tightly controlled by the account custodian.

d. The account custodian may assign members (including Postal Service employees and contractors) to shared accounts, who should be the sole users of the account. Shared accounts have a single log-on ID that is used by more than one individual. The managed e-mail account may only be created on the usps.gov domain.

e. When a special account is accessible by more than one individual, those individuals (i.e., registered members in eAccess/ARIS) must be registered, approved and reviewed periodically by the account custodian and/or custodian's manager.

9-3.2.11 Emergency Access when Individual is not Available

In instances during which an individual has possession of Postal Service information that is required by his or her manager and the individual is unavailable (e.g., on annual leave), the following process must be followed:

a. The individual's manager initiates a request for access to the information using a documented procedure (e.g., remedy or information ticket). The individual's manager is accountable for the emergency access.
b. Audit logging for all activities related to an emergency access request is required and must be protected and retained according to Postal Service standards.
c. The emergency access must be conducted under the identity of the user authorized by the manager and actually performing the access. Under no circumstance will the unavailable individual's log-on ID or password be used or compromised in an emergency access.
d. The system administrator either rewrites the access rules giving the manager or the manager's designee access to the information (files), or

the system administrator is authorized by the manager to access the information on the manager's behalf.

e. Upon completion of the emergency access, all access to the information is returned to its original state.

f. The unavailable individual is notified of the emergency access as soon as he or she becomes available.

9-3.2.12 Emergency Access to Production Information

In instances during which a developer or database administrator needs emergency (e.g., after hours) access to production information, the following process must be followed:

a. The individual opens a remedy ticket. The individual is accountable for the actions performed during the emergency access.

b. Audit logging for all activities related to an emergency access request is required and must be protected and retained according to Postal Service standards.

c. The emergency access must be conducted under the identity of the individual actually performing the access.

d. Upon completion of the emergency access, all access is returned to its original state.

e. The remedy ticket is closed.

9-3.3 Authorization Requirements

Access to internal information resources must comply with authorization requirements including, but not limited to, the following:

a. The information resource must not allow access to resources without invoking the authorization process and checking the assigned rights and privileges of the authenticated user.

b. The information resource must have features to assign user privileges (i.e., access permissions) to log-on IDs, roles, groups, and information resources.

c. Privileges on information resources (e.g., computing devices, consoles, terminals, and subsidiary networks) must not allow the user to bypass or upgrade his or her privileges established in centralized access control lists or databases.

d. The information resource must have the capability to restrict session establishment or information resource access based on time of day, day of the week, calendar date of the login, and source of the connection. Information resources running on operating systems that do not have these capabilities must implement compensating controls (e.g., monitoring devices).

e. The information resource must provide the administrator-configurable capability to limit the number of concurrent log-on sessions for a given user.

f. The information resource must not offer any mechanism to bypass authorization restrictions.

g. Access granted to the information application resource must be accurately reflected in eAccess/ARIS and should not extend beyond the pre-established role definitions.

h. Computing devices, mobile or otherwise, requesting access from remote, non-Postal Service locations must authenticate before access is granted.

External Access compliance instructions are as follows:

a. For information resource accesses that require authorization, the information resource must not allow access to resources without invoking the authorization process and checking the assigned rights and privileges of the authenticated user. Not all information resources require authorization; some only require authentication.
b. The information resource must have features to assign user privileges to User IDs based upon, roles, user services, company records, and related information resources.
c. Privileges on information resources (e.g., data sets, online pages/URLs, functions, etc.) must not allow the user to bypass or upgrade his or her privileges established in centralized customer databases.
d. The information resource must have the capability to enable access to external users 24 hours a day, 7 days a week.
e. The information resource must not offer any mechanism to bypass authorization restrictions.
f. Access granted to the information application resource must be accurately reflected in the customer's external account and should not extend beyond the pre-established authorization privileges and definitions. Some form of authentication must proceed authorization approvals.

9-4 Accountability

Accountability is the process of associating any action on the information resource with one and only one user, process, or other information resource and is essential for maintaining minimum levels of information security.

9-4.1 Types of Accountability

Accountability for access to information resources must be established at the site, network, and the individual level.

9-4.1.1 Site Accountability

Site accountability associates users or information resources with a specific location. Site accountability is established by issuing a site identification number or code (site ID) that is restricted by system hardware or software to a unique system, network, or terminal address in a controlled environment.

9-4.1.2 Network Accountability

Network accountability associates users or information resources with a specific network or logical subnet to a network. Network accountability is established by issuing a network identification number or code (network ID) or through the network address.

9-4.1.3 Individual Accountability

Individual accountability associates each user or information resource (e.g., a workstation or terminal) with any action on an information resource. Individual accountability is established by issuing a unique user or log-on identification number or code (i.e., user ID or log-on ID). Machine accountability may be established for a specific information resource through its workstation address or other identifier. All information resources must be capable of individual accountability and must do the following:

a. Identify information resources each time they attempt to log-on to the system.

b. Verify that information resources are authorized to use the system.

c. Associate all actions taken by an information resource with that resource's unique identifier (i.e., resource ID or log-on ID).

9-4.2 Types of Accounts

Internal users (workforce) – Access to information resources is managed through the use of multiple types of accounts, including the following:

a. User.

b. Privileged.

c. Service.

d. Shared.

e. Vendor default and vendor maintenance.

f. Guest.

Ownership for privileged, shared, and maintenance log-on IDs must be documented and administered in a secured manner.

For a complete description of accounts, refer to 9-4.2.1 through 9-4.2.6.

External users (customers):

a. Personal User – Used for external users who have a customer username and password.

b. Business User – Used for external users (who declared themselves a business user) who have a customer username and password.

c. Pending (upgradeable to full account) – Used to track external users who do not have a customer username and password but do have some privileged interaction with a Postal Service information resource.

d. Partial (not upgradeable to full account) – Used to track external users who do not have a customer username and password but do have some privileged interaction with a Postal Service information resource.

9-4.2.1 User Accounts

User accounts provide application/platform users with a minimum level of information resources and application functionality needed to perform their

duties (i.e., least privilege) and do not carry special privileges above those required to perform the user's business function. This includes limited access accounts that exist for a specific purpose (e.g., an auditor account).

Application user accounts are used to log into the application via a front-end interface, and the account privileges and roles are restricted by the approved access. Platform user accounts (i.e., database and operating system) are used to access platform-level resources and are limited to non-privileged access rights.

9-4.2.2 Privileged Accounts

Privileged accounts (e.g., administrator or maintenance accounts) are accounts that allow entitled users access to change data, alter configuration settings, run programs, or permits unrestricted access to view data. Assignment must be restricted to a unique individual whose duties require these additional privileges (e.g., system, network, database administrators). Use is restricted to performing those job functions required by the privileged account (e.g., creating new user profiles or altering the rights of existing non-privileged users); individuals must use their regular user accounts to perform non-privileged functions such as Internet access and Postal Service email.

Privileged accounts include Enterprise Admins, Schema Admins, Domain Admins, Administrators, Account Operators, Server Operators, Print Operators, and Backup Operators. Permission inheritance must be disabled for all privileged accounts.

Privileged uses must use two-factor authentication. An audit trail must be maintained on all privileged account usage.

Application accounts must not have the capability to run as "root."

9-4.2.3 Service Accounts

Service accounts are assigned to an information resource (e.g., server, application) or other automated process/service (not an individual) used to process data and/or identify actions or requests. Normally, the operating system uses this account when it hosts a service. Service accounts must be placed under management control. Service accounts must be created with the minimum access rights and privileges required to perform the necessary business function. These accounts must not be allowed root or administrative privileges. They are managed by the Postal Service entity responsible for the life cycle of the account from creation, deployment, usage, and retirement when no longer needed. See 9-6.1.8, Requests for Use of non-expiring Service Accounts for use of service accounts with non-expiring passwords.

9-4.2.4 Shared Accounts

There are two types of shared accounts:

a. Shared accounts (e.g., training accounts) have a single log-on ID and password that is used by more than one individual. A shared account must be used only for qualifying circumstances and when deemed necessary by the CISO. This approach to account usage is highly discouraged and requires the appropriate level of management approval via eAccess/ARIS as well as approval by the CISO. The use of shared accounts must be tracked (e.g., logged) to manage individual accountability. The requesting manager is responsible for

undocumented usage of the shared accounts and is responsible for password management. Shared accounts must not include access to Postal Service production systems, the Internet or the PCI environment. System operators must not share identification or authentication materials of any kind, nor allow any other person to operate any information systems by employing that user's identity. Generic accounts must not be used to administer PCI system components.

b. Managed email accounts are used to provide a single email mailbox that can be shared by multiple users. This mailbox is in addition to their personal regular mailboxes. The account is controlled by the account custodian. The custodian must send an email to the Postal Service Special Account Administrator to request access for a user. "Send As" allows a user to send emails from the name of the mailbox. The password is never shared and each user logs on to his or her workstation with his or her own User ID and password.

9-4.2.5 Supplier and Vendor Default and Maintenance Accounts

Supplier and vendor default accounts are accounts that are pre-installed on a product and must be removed or disabled. Supplier and vendor maintenance accounts are user accounts for the maintenance of their products to resolve issues related to the product and must be enabled only when needed, monitored, and controlled by a responsible Postal Service organization. Supplier and vendor maintenance personnel must not have access (including remote access) to any PCI cardholder data environment or PCI systems without documented business justification and CISO approval.

9-4.2.6 Guest Accounts

Guest accounts are not allowed for access to Postal Service network information resources. Guest accounts expose information resources to risk by allowing access to information resources through the use of a generic logon ID that either uses no password or a widely known password. Guest accounts incorporated into any software or established through any other means must be deleted or disabled. This policy does not apply to guest networks isolated from the Postal Service intranet that are used to support non-Postal Service external access.

9-4.3 Account Management

Internal Accounts (workforce) – Accounts must be established in a manner that ensures access is granted based on clearances, need to know, separation of duties, and least privilege basis. Accounts unused for 15 calendar days must be disabled.

Accounts unused for 1 year must be deleted. A user account suspension can also be triggered by certain clock rings in Time & Attendance System (TACS)

External users (customers):

a. Personal User – Used for external users who have a customer username and password.

b. Business User – Used for external users (who declared themselves a business user) who have a customer username and password.

c. Pending (upgradeable to full account) – Used to track external users who do not have a customer username and password but do have some privileged interaction with a Postal Service information resource.

d. Partial (not upgradeable to full account) – Used to track external users who do not have a customer username and password but do have some privileged interaction with a Postal Service.

e. Personal or business accounts unused for more than 400 days may be disabled. Unused accounts are not deleted. Pending account options to upgrade to a full account are only valid for 15 calendar days and then disabled.

9-4.3.1 Establishing Accounts

Internal Users (workforce):

To establish an account, personnel must request an account from their manager or supervisor via eAccess/ARIS at *https://eaccess.usps.gov.*

External Users (customers):

External users may sign up for an external account as needed, and without additional approval by anyone in the Postal Service.

9-4.3.2 Documenting Account Information

Internal accounts (workforce):

The account information, or database, must contain the following information for each user account: log-on ID, group memberships, access control privileges, authentication information, and security-relevant roles. Any security-related attributes that are maintained must be stored securely to protect their confidentiality and integrity.

External accounts (customers):

The account information shall be centrally managed via the customer's external account. Information about the account must include the following information, Username, User ID, membership details, access controls, levels of assurance, date/time of registration as well as IP address, authentication information and authorization data. Any security related attributes that are maintained must be stored securely to protect their confidentiality and integrity.

9-4.3.3 Configuring Account Time-Outs

Internal Accounts (workforce)– Accounts must be configured to log the workstation off the network or disable the session after a predetermined period of inactivity and enforce re-authentication. This requirement should be automated where possible. The Postal Service default standard period of inactivity is a maximum of 30 minutes. This action reduces the amount of time Postal Service information resources are vulnerable to compromise. Any deviation from this standard is the responsibility of the executive sponsor and must be documented and approved by the CISO.

External users (customers) – The session time-out period due to inactivity for external accounts is 15 minutes.

9-4.3.4 Local Accounts

All access to information resources will be through Active Directory accounts/ passwords or Active Directory enforced two-factor authentication protocols. Local accounts are prohibited on all servers, workstations, laptops, and other end-user computing devices (this prohibits the creation of new local accounts and requires the removal of any existing local accounts from the aforementioned resources). Users and operations staff will use individually issued and identifiable Active Directory accounts for access.

Exceptions to this policy are the following:

a. The local built-in administrator account will be retained on all servers, workstations, and laptops but is restricted to operations personnel working on servers or workstations that are disconnected from the network and unable to authenticate to the directory. The local built-in administrator accounts and their passwords will be maintained in accordance with requirements for elevated privileged accounts. These accounts are part of the standard server build/configuration and do not require separate approval or management through eAccess/ARIS.

b. Mobile computing device access is granted a blanket exception as the current models are restricted to local accounts only. These accounts are part of the standard device build/configuration and do not require separate approval or management through eAccess/ARIS.

Other exceptions may be granted on case-by-case bases by the CISO and the manager IT Desktop Computing (ITDC) where a COTS product will not work without a local account or there is a compelling business or operational need.

Requests for exceptions to the policy prohibiting local accounts other than the built-in Administrator and mobile computing devices accounts must be made through eAccessARIS. The approving manager must be a PCES manager; CISO will be the FSC; and ITDC will be the log administrator. The eAccess/ARIS system serves as the archive for requests, approvals/denials, and implementation if approved.

9-4.3.5 Departing Personnel

Accounts must be deleted or passwords changed when personnel leave the organization.

9-4.3.6 Vendor Maintenance Accounts

Vendor maintenance accounts must be managed, enabled only when needed by the vendor, and monitored while being used.

9-4.3.7 Handling Compromised Accounts

Internal users (workforce):

Information resources must provide automated mechanisms to support identifying and handling information security incidents. All personnel who

suspect an account has been compromised must immediately notify management and follow the incident reporting process (see 13-3.2, Incident Reporting).

External users: (customers):

All personnel who suspect an account has been compromised must notify eSAFE, the Inspection service and the CISO Threat Intelligence Team.

9-5 Identification

Identification is the process of associating a person or information resource with a unique enterprise wide identifier (e.g., a user log-on ID). The log-on ID is used in conjunction with other security services, such as authentication measures, to track activities and hold users accountable for their actions. Users are responsible for all actions performed on Postal Service information resources under their log-on ID.

Internal users (workforce): Identification requirements for processing and control devices in the mail processing and mail handling equipment (MPE/MHE) environment for private non-routable network address space are defined by Engineering.

External users (customers): Online user activity will be tracked based upon a digital identity. Digital identity is the online persona of a subject and is the unique representation of a subject engaged in an online transaction.

9-5.1 Issuing Log-on IDs

Log-on IDs or user IDs are unique groups of letters, numbers, or symbols assigned to a specific person or information resource.

Internal users (workforce): All personnel using Postal Service information resources are issued a log-on ID in conjunction with the authorization process. No two users are assigned the same log-on ID. This policy does not apply to users of managed shared accounts.

External users: (customers): Users creating an external account will be issued a User ID (a number) which will be related to their login or username. No two users are assigned the same log-on ID.

9-5.2 Protecting Log-on IDs

Log-on IDs must be protected in accordance with the following:

a. Personnel must not share their log-on IDs or permit others to use them to access Postal Service information resources.

b. Log-on IDs must not be embedded in application code or batch files or stored in application files or tables unless approved compensating security controls are implemented.

9-5.3 Suspending Log-on IDs

Internal users (workforce) – After six unsuccessful attempts to log on to an information resource, the log-on ID or account must be disabled for a period of at least 5 minutes (or 30 minutes for PCI-related applications or until the system administrator resets the account). If the log-on ID or account does not unsuspend itself after the suspension period, the user must use ePassword Reset or call the Help Desk and follow defined procedures for resolution.

Employees who remain in a Leave Without Pay (LWOP) status for a period in excess of 15 calendar days, or who are expected to be in a LWOP status in excess of 15 calendar days, must have their eAccess/ARIS account disabled until such time as they return to an in-work status.

In addition, customers have an option to recover username, if forgotten.

External users (customers) – For externally facing login pages, do as follows,

a. After 5 unsuccessful attempts to log on to a customer's managed login page, the user needs to wait 1 minute until they can attempt to login again.

b. With 3 additional unsuccessful attempts, the user will be prompted to wait 5 additional minutes.

c. With 2 additional unsuccessful login attempts (total of 10), the user will be prompted to wait 15 minutes until their next attempt.

d. With 1 additional unsuccessful login attempt (#11), the user will be prompted to wait 30 minutes.

e. With the 12th unsuccessful login attempt, the user will need to wait 1 hour.

f. With the 13th unsuccessful login attempt, the user will need to wait 24 hours until they can login again.

g. For all other customer -related login pages, after 4 unsuccessful login attempts, the user will not allowed to login again for 24 hours. In both cases (customer -owned login page and customer -related login page), customers can also use the I Forgot My Password process to access their account.

9-5.4 Failed Log-on Attempts

9-5.4.1 Recording Failed Log-on Attempts

Failed log-on attempts must be recorded for audit trail and incident reporting purposes.

9-5.4.2 User Notification of Failed Log-on Attempt

Notification to the user of a failed log-on attempt will reflect only that the logon failed. The reason for the failed log-on attempt and information previously entered, including the disguised or clear password, must not be returned to the user.

9-5.5 Terminating Log-on IDs

Internal users (workforce)–Log-on IDs not used for the last 365 days must be deleted.

External users (customers) – Log-on IDs not used in the last 365 days must be deleted.

External users (customers) – External accounts are not deleted for non-use.

9-5.6 Identification Requirements

Internal users (workforce) :

Information resources must comply with security requirements including, but not limited to, the following:

a. The information resource must, at a minimum, use log-on IDs as the primary means of identification.

b. The information resource must have the capability to automatically disable a log-on ID that has not been used for an administrator configurable period of time.

c. The information resource must not allow an administrator to create, intentionally or inadvertently, a log-on ID that already exists.

d. A log-on ID must not exist without associated authentication information.

e. The information resource must not provide any process to bypass the authentication information for any log-on ID.

f. The information resource must have the capability of associating each internal process with the log-on ID of the user who initiated the process. Processes that are not initiated by a user, such as print spoolers, database management servers and any spawned sub-processes, must be associated with an identifier code, such as "system ownership."

External users (customers):

a. The information resource must, at a minimum, use User IDs as the primary means of identification of a user's account.
b. The information resource must have the capability to disable an account that has not been used for an administrator-configurable period of time.
c. The information resource must not allow an administrator to create, intentionally or inadvertently, a unique account that already exists.
d. A User ID can exist without associated authentication information.
e. The information resource must not provide any process to bypass the authentication information for any log-on ID.
f. The information resource must have the capability of associating each on-line activity with the User ID of the user who initiated the process.

Internal Users (workforce): Authentication is the process of verifying the claimed identity of an individual, workstation, or originator. While identification is accomplished through a logon ID, authentication is achieved when the user provides the correct password, personal identification number (PIN), or other authenticator associated with that identifier. Internal users or personnel must be required to identify and authenticate themselves to the information resource before being allowed to perform any other actions.

External users (customers):

Digital authentication establishes that a subject/claimant attempting to access a digital service is in control of the technologies used to authenticate. This approach supports privacy protection by mitigating risks of unauthorized access to individual's information. Authentication of a user's account may occur via username/password, or via username in conjunction with shared secrets or via synchronized access tokens. Location and device identity are not considered authentication factors.

Access to any database containing cardholder data must be authenticated. This includes access by applications, systems and database administrators, and users. Direct access and queries to PCI databases must restricted to database administrators and must be logged.

Authentication requirements for processing and control devices in the MPE/ MHE private non-routable network address space are defined by Engineering.

Means of authentication, or authenticators, may include the following:

a. Passwords.
b. Personal identification numbers.
c. Shared secrets.
d. Digital certificates and signatures.
e. Smart cards and tokens.
f. Biometrics.
g. Strong authentication.

9-6.1 Passwords

Passwords are unique strings of characters that personnel or information resources provide in conjunction with a log-on ID to gain access to an information resource. Passwords, which are the first line of defense for the protection of Postal Service information resources, must be treated as sensitive information and must not be disclosed.

9-6.1.1 Password Selection Requirements

Password requirements must comply with the following:

Internal application users (workforce): – Password requirements must comply with the following:

a. For all users, passwords for all platforms except mobile devices must consist of at least 15 characters and contain at least one character from three of the four following types of characters: English uppercase letters (A–Z), English lowercase letters (a–z), Westernized Arabic numerals (0–9), and nonalphanumeric characters (i.e., special characters such as &, #, and $).

b. Password requirements associated mobile devices will be based on the capability of the hardware and software and can be found in the appropriate policy/procedure documents.

c. The only nonalphanumeric characters available for the mainframe are: @, #, and $.

d. For all users, passwords must not contain the user's name or any part of the user's full name.

e. Passwords must not be repeated (reused) for at least five generations.

External application users (customers; *www.usps.com*, Business Customer Gateway, and related applications) – Password requirements must comply with the following:

a. Passwords must consist of at least 8 characters and contain at least one upper case character (A-Z), one lower case character (a-z), and one number (0-9). Special characters are allowed but are limited to the following: – ().&@?',/"+!).

b. The password must not contain more than 2 consecutive repeat characters.

c. Passwords cannot match the username.

9-6.1.2 Password Selection Recommendations

The following password recommendations are prudent security practices intended to enhance the password complexity and protect the password from attempted password cracking:

a. Do not use family member names or other information easily discovered about the user (e.g., license plate number, phone number, birth date, and street name).

b. Do not use commonly used words such as words that appear in the dictionary or Postal Service terminology.

c. Do not use all the same characters or digits or other commonly used or easily guessed formats.

d. Use longer password conventions whenever possible (e.g., passphrases and run-on multiword strings).

e. Do not use all the same characters or digits or other commonly used or easily guessed formats, such as: a1a1a1a1 or 123d123d.

f. To remember your passwords and make them stronger, instead of thinking in terms of pass 'words', think in terms of 'phrases', where your password is a short phrase separated by special characters or

numbers. Examples would be: Kick_the_can1; 4Jump-the-shark4; and Ocean5Sunset.

g. Use industry best practices (such as banking, FICAM) to determine allowable passwords.

9-6.1.3 Initial Password

Internal users (workforce): – Passwords must always be delivered in a secure manner. The initial password for users must be sent via protected electronic delivery system or personal delivery to the user (First Class Mail is also acceptable). For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at log-on.

Note: Caution must be taken not to use standard generic or global passwords when issuing new accounts or when resetting forgotten passwords.

9-6.1.4 Password Suspension

Internal users (workforce) – After six unsuccessful attempts to log on to an information resource, the log-on ID or account must be disabled for a period of at least 5 minutes for internal systems accessed via ACE and non-ACE devices, (or 30 minutes for PCI-related applications or until the system administrator resets the account).

External users (customers) – For externally facing login pages:

a. After 5 unsuccessful attempts to log on to a customer managed login page, the user needs to wait 1 minute until they can attempt to login again.
b. With 3 additional unsuccessful attempts, the user will be prompted to wait 5 additional minutes.
c. With 2 additional unsuccessful login attempts (total of 10), the user will be prompted to wait 15 minutes until their next attempt.
d. With 1 additional unsuccessful login attempt (#11), the user will be prompted to wait 30 minutes.
e. With the 12th unsuccessful login attempt, the user will need to wait 1 hour; with the 13th unsuccessful login attempt, the user will need to wait 24 hours until they can login again.
f. For all other customer -related login pages, after 4 unsuccessful login attempts, the user will not be allowed to login again for 24 hours.
g. In both cases (customer -owned login page and customer -related login page), customers can also use the I Forgot My Password process to access their account.

9-6.1.5 Reset Passwords

Internal users (workforce)– Users with non-privileged accounts who have forgotten their passwords or need to perform routine password resets, should reset their password by invoking ePassword Reset. The exception to using the ePassword Reset system is for privileged, machine and vendor default accounts (see below). The ePassword Reset system requires user authentication prior to allowing the user to perform a password reset. If a user calls the Help Desk to reset a password, users are challenged by Help Desk personnel to provide further confirmation of identity prior to resetting the password. Password change requests via the Help Desk are

documented via a change request ticket. The password is reset to a temporary password by an administrative group, and the user must then change the password at first log-on.

ePassword Reset is not used for privileged, machine, and vendor default accounts. The passwords to these accounts are changed by the system administrator group via the Help Desk. When users of these accounts request the reset of a password, the users are challenged by Help Desk personnel to provide further confirmation of their identity (e.g., some predetermined shared secret that only the user would know) prior to resetting the password. Upon confirmation of user identity, the request is documented via a change request ticket and assigned to the appropriate administrator group for resetting the password. For privileged accounts, the administrator group resets to a temporary password and the privileged user must then change the password at first log-on.

External users (customers) – For external users, passwords may be reset as follows:

a. Help-desk call. Users calling the help desk are challenged by helpdesk personnel to provide further confirmation of their identity prior to resetting the password. Upon confirmation of the user identity, the request is documented in the external users internal application. A temporary password can be sent by the help-desk personnel via email to the end user. Upon receipt, the user can type in their username and temporary password. Users will then need to enter a password into external users application to complete their login.

b. I Forgot My Password self-service process. External customers may reset their passwords via entering the answers to their secret questions into the external users page. If successful, the user will then be prompted to type in their new password to complete their login.

c. SMS Account Recovery. Customers who have signed up for account recovery via SMS codes can enter the code received by verification text or email on the webpage.

9-6.1.6 Password Expiration

Internal users (workforce)– The information resource must offer an authentication information-aging feature that requires users to periodically change authentication information, such as passwords. All Postal Service personnel must change their passwords when prompted by the system or risk being locked out, thus requiring assistance to reset the account. Password expiration requirements are as follows:

a. Prior to the expiration of authentication information, such as passwords, the information resource provides notification to the user.

b. At least every 30 days, passwords for privileged accounts or for those accounts considered sensitive (e.g., system supervisors, software specialists, system administrators, database administrators [DBA, SYSDBA, SYSOPER, INSERT ANY TABLE, UPDATE ANY TABLE, DELETE ANY TABLE], or vendor-supplied) must be changed.

c. At least every 90 days, passwords for all other accounts must be aged and changed.

Oracle database schema accounts are assigned to a database (not an individual) and are typically considered the application owner. These accounts have minimum access rights and privileges required to perform the necessary business functions with respect to the application. Oracle Database Schema Accounts closely resemble Service Accounts as they are not granted root or administrative privileges and are placed under management control [Database Systems and Services (DBSS) is the Postal Service entity responsible for the life cycle of the account from creation, deployment, usage, and retirement when no longer needed]. DBSS is responsible for password maintenance on all Oracle Database Schema Accounts. DBSS must take the following measures to protect the password:

a. The password is not provided to anyone outside of DBSS.
b. If the password is stored in a database, it is encrypted.
c. If the password is stored in a file, the file is protected.
d. If scripts need to be run as the schema account, DBSS staff enters the password.
e. The password for schema accounts must comply with a password strength function that enforces the password to be at least 15 characters long. This is necessary because the schema account password does not expire so extra measures are taken to protect it.
f. DBSS has monitoring in place on all databases for usage of this account and records all suspicious activity.

External users (customers) – There are no requirements for external customers to change their passwords on a periodic basis.

9-6.1.7 Requests for Use of Nonexpiring Password Accounts

All requests for use of nonexpiring password accounts must be approved by the manager, CISO. The manager CISO must be added as a FSC for all machine accounts. These accounts are tracked for compliance purposes. The executive sponsor is accountable for the use of these accounts. If approval is granted, the following compensating controls must be implemented:

a. Account must be in a centrally managed database. No privileged access allowed.
b. Encrypt the LDAP call to keep the password from being transmitted across the network in clear text.
c. Change password when personnel with access to the account leave or transfer.
d. Non-expiring password accounts must be requested and documented through eAccess/ARIS.
e. Ownership of non-expiring password accounts must be identified and recertified on a semi-annual basis.
f. Rights and privileges of non-expiring password accounts must be reviewed at least on a semi-annual basis to evaluate the appropriateness of access.
g. Passwords for non-expiring password accounts must use a complex password that exceeds standard length requirements.

h. Source-restrict the account to a specific host and do not allow console or remote entry.

i. Restrict access to the password to operations staff with a need to know.

9-6.1.8 Requests for Use of Non-expiring Service Accounts

All requests for use of non-expiring password service accounts must be submitted in writing (e-mail is acceptable) by the executive sponsor to the manager, CISO. The rationale for these accounts is to prevent service interruptions due to a locked account. These accounts must be tracked for compliance purposes. The executive sponsor will be held accountable for the implementation of these accounts. If approval is granted, the following compensating controls must be implemented:

a. Account must be requested and documented in eAccess/ARIS.

b. No privileged access allowed; specific ACL's must be applied under the concept of 'least privilege'. Use of root, system administration, non-cancel, etc. privileges are prohibited.

c. Account must not have the rights to modify or delete system (e.g., syslog or Windows System Event) or security log files.

d. Restrict account's usage to a specific host.

e. Direct login to the service account, whether from a console or remote session, is prohibited and must be disabled.

f. Rights and privileges of account must be reviewed and validated on a semi-annual basis.

g. Non-expiring password must meet Postal Service standards, including password length and complexity, and be encrypted in storage and in transit. The only exceptions to the criteria are password aging and account suspension on failed login attempts.

h. Restrict access to password to operations staff with a need to know and change when personnel with access leave or transfer. Comply with 6-6, Departing Personnel, to terminate all access when personnel leave or are transferred.

9-6.1.9 Password Protection

Passwords used to connect to Postal Service information resources must be treated as sensitive information and not be disclosed to anyone other than the authorized user, including system administrators and technical support staff. Requirements for protecting passwords include the following:

a. Passwords must not be shared except those used for shared accounts.

b. If passwords are written down and stored outside the user's personal control, they must be secured in a tamper-resistant manner (e.g., an envelope with registry seal, time stamped, and signed by the user) to ensure that any disclosure or removal of the written password is clearly recognizable.

c. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user or has been otherwise

compromised, the user must immediately change the password and notify CyberSafe.

d. Passwords must be encrypted in transit.

9-6.1.10 Password Storage

Passwords must be stored in one-way encrypted format where possible. There may be cases where business requirements for the system are unable to meet one-way encryption implementation, these exceptions should be identified and documented as part of the certification and accreditation process. Passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems must be encrypted using the Postal Service encryption standard documented in 9-7.1.1, Minimum Encryption Standards, and decrypted when used.

Passwords for external users may not be decrypted when used.

9-6.1.11 Vendor Default Passwords

Vendor-supplied default accounts must be disabled, removed, or the passwords must be changed before connecting the system or introducing the software to the Postal Service network. This includes passwords used by contractors or consultants when configuring a system.

9-6.1.12 Password Requirements

Internal users (workforce) – Information resources must support the following password requirements:

a. Deny access if the user does not comply with password selection or expiration criteria.

b. Set initial password to a temporary password and require user to change the temporary password on first log-on.

c. Suspend account after an administrator-configurable number of unsuccessful entries.

d. Require re-authentication by the user, as well as reconfirmation of the new password, at the time of an attempted password change.

e. Mask password entry during the authentication process.

f. Store passwords in a one-way encrypted format.

g. Encrypt passwords in transmissions.

h. Require users to change passwords (password aging every 90 days or when compromise is suspected).

i. Change vendor-supplied default passwords prior to use.

External users (customers):

Information resources must support the following password requirements:

a. Accept user created passwords that only comply with the password selection criteria.

b. Lock account after an administrator-configurable number of unsuccessful entries.

c. Require reconfirmation of the new password at the time of an attempted password change.

d. During the password entry process, allow one letter/character to be shown to the user as they type in the password and mask the previous entry after each subsequent password character is entered.

e. Store passwords in a one-way encrypted format.

f. Encrypt passwords in transmissions via HTTPS/POST.

g. Do not require users to change passwords on a periodic basis.

h. Enable a forced change to user passwords based upon a data breach or known fraudulent activities.

9-6.2 Personal Identification Numbers

PINs are a specialized type of authenticator that are used in conjunction with unique identifiers to verify the identity of users before allowing them access to information resources. Use Postal Service 4-digit PINs only for limited interfaces such as the Integrated Voice Response (IVR) based non-sensitive applications. Do not use Postal Service 4-digit PINs for Human Resource self-service web-based applications.

Where technologically capable, use of PINs with increased complexity are mandatory in order to meet challenges posed by increasing information security threats and developing technological advancements. Where technically capable, these PINs must include the following composite design: eight-character minimum combination of numbers, letters, and special characters, with a defined window for expiration.

Like passwords, PINs must be treated as sensitive information and must not be disclosed. All personnel must comply with Postal Service policies regarding PIN management and usage and are directly responsible for all actions taken using an assigned identifier and PIN.

9-6.2.1 PIN Generation and Selection Requirements

To ensure that PINs retain integrity and confidentiality, PINs must be protected during generation and dissemination. All personnel are encouraged to change their PIN from the initial assignment. PINs must:

a. Be a minimum of four characters in length, two of which are unique.

b. Avoid obvious combinations or sequences.

c. Avoid well-known or easily guessed combinations (e.g., social security number, telephone number, and house address).

9-6.2.2 PIN Distribution

Secure delivery methods include First Class Mail, an encrypted delivery system, or personal delivery to the user. New or replacement PINs must not be delivered by telephone, facsimile, or electronic mail to protect against unauthorized disclosure.

9-6.2.3 PIN Protection

PINs must be committed to memory or stored in a secure location. Information resources must store PIN data in an encrypted format that meets Postal Service encryption standards. All access, additions, modifications, and deletions to the PIN data must be logged and monitored. If PIN authentication is performed over an open network, such as the Internet, PINs

must be encrypted during transmission according to Postal Service encryption standards.

9-6.2.4 Forgotten PINs

When requesting replacement of a forgotten PIN, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes. All forgotten PINs must be replaced with securely delivered new PINs.

9-6.2.5 Suspension

When using a PIN for authentication, the information resource must be disconnected after three incorrect entries and the PIN account suspended after six incorrect entries. When a suspended PIN account is reactivated, the user must be assigned a new PIN that is delivered via secure methods.

9-6.2.6 PIN Cancellation and Destruction

A PIN suspected of compromise must be cancelled immediately and a new PIN generated and delivered via secure methods. Unauthorized users who no longer require access to the system must be removed immediately. All PIN data must be destroyed when the user no longer requires access to the system or leaves Postal Service employment.

9-6.2.7 PINs Used for Financial Transactions

PINs used for financial transactions must comply with American National Standards Institute Financial Services Technical Publication X9.8, PIN Management and Security. Financial transactions at high risk for fraud may not be suitable for reliance on PINs as the primary authentication mechanism.

9-6.3 Shared Secrets

A shared secret is an authentication mechanism used to re–set a user's password or PIN. When requesting the reset of a password or PIN, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes.

Internal users (workforce)– shared secrets must comply with the following:

a. Be a minimum of eight characters.

b. Be protected and stored as sensitive information.

c. Be stored encrypted if stored electronically.

d. Have the user's account disabled if the shared secret is entered incorrectly three times.

e. Ensure an information resource using shared secrets provides a secure process for recording an initial shared secret and changing the shared secret in the event of suspected compromise.

External users (customers):

a. Be a minimum of three characters.

b. Be protected and stored as sensitive information.

c. Be stored encrypted if stored electronically.

d. Do not allow changes to shared secrets.

9-6.4 Digital Certificates and Signatures

A digital certificate is an X.509 certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer, or service identity contained within the certificate. The certificate's purpose is to relate a unique name to a specific public key and is used for encryption and decryption of files and the nonrepudiation of messages. USPS sets standards for the properties, utilization, and acceptance of digital certificates in USPS systems and applications where digital certificates are used.

Cryptographically, X.509 is the standard defined by the public key certificate within USPS. As defined in 11-1.1.4, the Postal Service uses X.509 certificates for secure communication, including the TLS and SSL protocols. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual). When signed by a trusted certificate authority, someone holding that certificate can rely on the public key it contains to authenticate the identity presented therein.

An X.509 is defined by the International Telecommunications Union's Standardization sector (ITU-T), and is based on ASN.1, another ITU-T standard and contains information about the identity to which a certificate is issued and the identity that issued it. Standard information in an X.509 certificate includes the following:

a. Version – which X.509 version applies to the certificate (which indicates what data the certificate must include).

b. Serial number – the identity creating the certificate must assign it a serial number that distinguishes it from other certificates.

c. Algorithm information – the algorithm used by the issuer to sign the certificate.

d. Issuer distinguished name – the name of the entity issuing the certificate (usually a certificate authority).

e. Validity period of the certificate – start/end date and time.

f. Subject distinguished name – the name of the identity the certificate is issued to.

g. Subject public key information – the public key associated with the identity.

h. Extensions (optional).

Within the Postal Service, the CISO determines the eligibility of each proposed role, group, code signer, system, application, or device to receive one or more certificates. The CISO determines and verifies the identity of the human sponsor for each proposed role, group, code signer, system, application, or device to receive one or more certificates

9-6.4.1 Digital Certificate

A digital certificate contains a public key and a private key. Digital certificates are used for identity verification prior to performing a separate action [by way of another process entirely, such as the Transport Layer Security (TLS) protocol] to transmit data securely. The Postal Service sets 9-6.4.2

standards for the properties, utilization, and acceptance of digital certificates in Postal Service systems and applications where digital certificates are used.

A public key certificate is a digitally signed document that serves to validate the sender's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (which may be either a user or a system name) and the holder's public key, as well as the digital signature of a certification authority for authentication. The certification authority attests that the sender's name is the one associated with the public key in the document. A user ID packet, containing the sender's unique identifier, is sent after the certificate packet. There are different types of public key certificates for different functions such as the following:

Device:

a. Web server SSL.

b. IPSEC tunneling.

c. Active directory authentication.

d. Data servers.

e. Secure terminal services.

f. Code signing.

g. Secure LDAP.

User:

a. PIV identification cards.

b. Client authentication.

c. Document signing and encryption.

d. Secure E-mail.

e. Encrypted file system (EFS).

9-6.4.2 Digital Signature

A digital signature is a digital code that can be attached to an electronically transmitted message or file that uniquely identifies the sender. The signature is used to authorize action, to demonstrate responsibility, and legally to indicate intent of decisions. Digital signatures enable electronic approvals promoting business efficiencies. Digital certificates are required when using digital signatures. Digital signatures perform three important functions:

a. Integrity allows the recipient of a given message or file to detect whether that message or file has been modified.
b. Authentication makes it possible to verify cryptographically the identity of the person who signed a given message.
c. Nonrepudiation prevents the sender of a message from later claiming that they did not send the message.

9-6.4.3 Certificate and Signature Standards

Certificate Authority (CA) operating requirements are defined within this policy, and may also be well-defined within a Certificate Policy (CP) document. This includes digital certificate properties, as well as utilization and acceptance. Certificate Authority server operational practices are defined within the Security Plan document for each Enterprise Information Repository (EIR) at the Postal Service that operates the Certificate Authority

(CA) servers, and may also be well-defined within Certificate Practice Statement (CPS) documents. If used, CPS documents are required for each CA Server and are used to describe how each of those CA servers are operated in accordance with the relevant CP document under which they must function.

9-6.4.4 Digitized Signatures

A digitized signature is a handwritten signature reproduced in its identical form as a TrueType font or graphical image. The signature may be embedded in electronic messages or documents as a representation of an individual's signature. There are no security associations with a digitized signature, e.g., non-repudiation and document integrity.

9-6.4.5 Certificate Stores

A Certificate Trust Store is a permanent storage where a Public Key Infrastructure (PKI) stores its certificates, CRLs, and certificate trust lists. A trusted root certificate is the cornerstone and trust anchor of authentication and security on the Internet.

Vendors' products come pre-populated with many root certificates in their trust stores, potentially certificates that Postal Service does not want to implicitly trust. The CISO sets the direction of what should be included in the trust stores and the Public Key Infrastructure Management Authority (PKIMA) provide technical assistance to application and system owners with regards to the content of installed product's trust stores through automated or manual processes, to include the following:

a. Removing all certificates that have passed their expiration date.

b. Removing all certificates that are no longer trusted.

c. Removing all certificates that are no longer required.

9-6.4.6 Naming Constraints

Names for certificate issuers and certificate subjects are of the X.500 Distinguished Name (DN) form. The "United States Postal Service" is a registered name in accordance with American National Standards Institute. The U.S. National Name Registration Authority uses of this identifier within USPS are not restrictive because the identifier is unambiguous and may be used in a variety of environments and various encoding methods. To be unambiguous, USPS must establish context and naming hierarchies. A single naming hierarchy is established within the Postal Service as outlined below:

a. Names for certificate issuers (i.e., USPS CA) and certificate subjects (i.e., subscriber or end entity) are of the X.500 DN form. These names are unique and unambiguous within the USPS hierarchy.
b. Certificate issuers have entries at the organization name level. The DNs follow the following form: OU=United States Postal Service, O=U.S. Government, C=US.
c. Certificate subjects have entries at the organizational Unit Name level. The DNs must follow the following form: CN=Subscriber Name, OU=United States Postal Service, O=U.S. Government, C=US.

Certificate subjects choose an optional Alternated Subject Name if marked noncritical. Certificate subjects choose to have additional name forms, such

as an e-mail address; however, the DN is the primary name and the one used to populate the subject fields of certificates and CRLs. Additional objects outside the scope of this policy must also be present in the naming hierarchy.

9-6.4.7 Meaningful Names

All names, including machine names and application names, are unique and understandable to humans. The DN must represent the subscriber in a way that is easily interpretable. For people, this is a legal name. For equipment, this is a model name and serial number. Distinguished names must be unique for all end entities of the USPS CA. X.500 DNs are used, and the USPS CAs enforce name uniqueness within the X.500 name space for which they have been authorized. When name forms other than a DN (e.g., e-mail address or DNS name) are used, they too are allocated to ensure name uniqueness.

The contents of each certificate Subject and Issuer name field have an association with the authenticated name of the Entity. A certificate issued for a device or application must include, within the Directory entry, the name of the person or organization responsible for that device or application. All certificates have name constraints asserted that limit the name space of the CAs to that appropriate for the domain.

9-6.4.8 Rules for Constructing Various Name Forms

Name forms are contained in the applicable certificate profile. As the USPS organization responsible for management and operation of the USPS X.500 directory. The Information Technology Engineering and Architecture (ITEA) group is responsible for the USPS X.500 directory name space and works with the Change Management Process for naming approval prior to final certificate provisioning.

9-6.4.9 Name Claim Dispute Resolution Procedure

Any dispute related to a name claim between USPS and an organization or individual outside of USPS is resolved using the following dispute settlement mechanism:

a. A dispute is resolved by negotiation if possible.

b. A dispute not settled by negotiation is resolved through arbitration by the USPS PKIPA.

9-6.5 Smart Cards and Tokens

Smart cards and tokens are tangible objects that usually contain a built-in microprocessor to store and process information used to verify the identity of a user. Smart cards and tokens are valid methods of authentication. The CISO must approve all implementations of these technologies for accessing information resources. The CISO, in conjunction with the Inspection Service, sets standards for the use and protection of smart cards and tokens. All personnel must protect smart cards and tokens from theft and not allow others to use them.

9-6.6 Biometrics

Using biometric information is a valid method of authentication. Biometrics are technologies used to authenticate individuals by means of unchanging biological characteristics (e.g., fingerprints, palm prints, voice prints, or facial, iris, and retina scans). The CISO must approve all implementations of biometric technologies for accessing information resources. Biometric information is sensitive-enhanced information and must be protected. The CISO, in conjunction with the Inspection Service, sets standards for the use of biometric authentication and the storage of biometric information.

9-6.7 Strong Authentication

Strong authentication consists of two-factor or multifactor authentication tools (e.g., smart card and PIN or thumbprint and password) that move toward the concept of nonrepudiation or conclusive tracing of an action to an individual. Single-factor authentication tools such as log-on IDs and passwords do not provide strong authentication.

Strong authentication is required for external native apps that are downloaded via an APP Store, such as Google PlayStore or ITunes. Native apps will encrypt the payload. Native apps will use two factor authentication to establish an encrypted channel through which payloads are communicated.

9-6.8 Nonrepudiation

Nonrepudiation is the security property that ensures that the sender cannot deny sending the message, the recipient cannot deny receiving the message, and actions can be conclusively traced to a specific individual. When required, an information resource must have the capability to support nonrepudiation.

A single public/private key pair and its associated certificate issued to any device may be used for signing (including authentication), key management (for encryption), or both. Device certificates must not assert nonrepudiation as well; all subscriber private keys must not be used by more than one entity.

9-6.9 Remote-Access Authentication

Postal Service information resources must support and maintain access control for personnel using networked, and Internet connections to Postal Service information resources. Strong authentication or other stringent access controls must be implemented for personnel entering through the Internet, or other non-Postal Service communication networks. Source restrictions (i.e., destination verification of remote session source address) may be used as a substitution to strong authentication for remote access. Two-factor authentication is required for remote access to PCI cardholder data.

Multifactor authentication is required for remote access to sensitive, sensitive-enhanced, and PCI cardholder data. Application owners centrally manage all remote access connections to their systems and ensure that remote access capabilities provide strong multi-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. All remote access connections must support cryptographic based, multifactor

authentication. Any multifactor authentication is based on USPS-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions must comply with the encryption requirements of FIPS 140-2, Level 3, and Security Requirements for Cryptographic Modules.

9-6.10 Session Management

A computer session is a unique period of activity performed on or by an information resource usually associated with a login by a user. All information resources must implement session management standards specific for the information resource platform.

9-6.10.1 Session Establishment

Internal users (workforce)– Information resources must comply with session establishment requirements including, but not limited to, the following:

a. During a login, the information resource must allow the entire login sequence to be completed before providing any response to the initiator of the login.

b. The information resource must generate an alarm after an administrator-configurable number of consecutive incorrect login attempts across multiple accounts.

c. When the threshold for invalid consecutive attempts (normally six) for a given log-on ID is reached, the information resource must deactivate access for the log-on ID for a period of at least 5 minutes (or 30 minutes for PCI-related applications or until the system administrator resets the account).

d. Upon successful session establishment, the information resource must make available the date and time of the last successful login.

External users(customers):

a. During a login, the information resource must allow the entire login sequence to be completed before providing any response to the initiator of the login.

b. The information resource must generate an alarm after an administrator-configurable number of consecutive incorrect login attempts across multiple accounts.

For externally facing login pages:

a. After 5 unsuccessful attempts to log on to a customer managed login page, the user needs to wait 1 minute until they can attempt to login again.

b. With 3 additional unsuccessful attempts, the user will be prompted to wait 5 additional minutes.

c. With 2 additional unsuccessful login attempts (total of 10), the user will be prompted to wait 15 minutes until their next attempt.

d. With 1 additional unsuccessful login attempt (#11), the user will be prompted to wait 30 minutes.

e. With the 12th unsuccessful login attempt, the user will need to wait 1 hour; with the 13th unsuccessful login attempt, the user will need to wait 24 hours until they can login again.

f. For all other customer -related login pages, after 4 unsuccessful login attempts, the user will not allowed to login again for 24 hours.

g. In both cases (customer -owned login page and customer -related login page), customers can also use the I Forgot My Password process to access their account.

Upon successful session establishment, the information resource must make available the date and time of the last successful login.

9-6.10.2 Session Expiration

Information resources must comply with session expiration requirements including, but not limited to, the following:

a. After the specified period of inactivity during the session (applicable standards defined by the manager, CISO ISS), the information resource must terminate the session and connection and require a successful re-authentication to regain access.

b. Following termination by the user or interruption by a power failure, system crash, or transmission problems, the session and connection must be dropped. The establishment of a new session requires the normal user identification, authentication, and authorization.

c. The information resource must provide an administrator-configurable session expiration (i.e., session lifetime). After the specified period of time, regardless of activity, the information resource must terminate the session, lock out the connection, and require a successful re-authentication to regain access.

9-6.10.3 Time-Out Requirements (Re-authentication)

The inactivity time-out standard for Postal Service information resources is a maximum of 30 minutes with the following exceptions:

a. For end-user devices and consoles associated with PCI applications, servers, and network devices the maximum is 15 minutes.

b. For conference rooms used for presentations the maximum is 2 hours.

c. For executives at the vice president level or higher the maximum is 2 hours.

d. For external end users (associated with a customer login), the maximum is 15 minutes.

After the maximum of period of inactivity, the information resource must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password. Any deviation from these requirements must be approved by the manager CISO and the executive vice president/CIO.

Manual re-authentication must be required before access to the information resource is re-established. For remote access, the session must be terminated and the information resource disconnected from the network.

Note: Use the Postal Service standard or refer to the specific platform configuration standards for the applicable time-out requirements.

9-6.10.3.1 End User Computing Devices

Internal users (workforce) – After the maximum period of 30 minutes of inactivity, the time-out event must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password. Manual re-authentication must be required before access to the end user computing device is reestablished.

External users (customers) – After the maximum period of 30 minutes of inactivity, the user will be required to log-in again to re-establish a new session. The establishment of a new session requires the normal user identification, authentication, and authorization.

9-6.10.3.2 **Applications**

After the maximum of period of inactivity define above, the application must time-out.

9-6.10.3.3 **Remote Access**

For remote access, the communications session is limited to 2 hours. After 2 hours, the end user computing device is asked to re-authenticate to the network. The normal end user computing device inactivity time-out standard described above applies.

9-6.10.3.4 **Failed Access Attempts**

Failed access attempts and access attempts by unauthorized personnel or information resources must be rejected and recorded for audit trail and incident reporting purposes.

9-6.11 Single Sign-On

Single sign-on (SSO) is the automated authentication for additional systems after the user has logged on once. The authenticating system passes the user information to the subsequently called system. This is done in the background; that is, the user does not need to authenticate himself or herself again after his or her first log-on. Certificate-based, two-factor authentication is required to ensure the identity of users accessing the sensitive information within SSO environments. All SSO initiatives must be implemented according to the architectural plan to ensure seamless integration within the enterprise and to avoid the establishment of isolated, unsupported islands.

9-6.12 Authentication Requirements

All information resources must comply with authentication requirements including, but not limited to, the following:

a. The authentication process should protect the information resource from a replay attack.

b. During information resource recovery, authentication information must be recoverable without unauthorized disclosure or loss of data and information resource integrity.

c. The information resource must support a configuration capability that prevents authentication information (e.g., password, PIN number, token, or smart card) from being displayed in clear text or otherwise made available to any other user, including an administrator.

d. When the initial authenticator is created, the information resource must not divulge the authenticator to anyone other than the user and the authorized administrator.

e. The information resource should have the ability to authenticate itself to the user and to other software application components during the authentication sequence.

f. Where technically feasible, information resources must support process-to-process authentication.

g. Failed log-on attempts must be recorded for audit trail and incident reporting purposes.

9-7 Confidentiality

Confidentiality is the security property that ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Information resources must have the capability to ensure that information is transmitted and stored in a way such that only authorized users are allowed access. Confidentiality is maintained through comprehensive and interrelated efforts that include, but are not limited to, the following: a. Information designation.

b. Clearances and need to know.

c. Physical security.

d. Authentication of users.

e. Encryption.

9-7.1 Encryption

Encryption is the primary means for providing confidentiality services for information that can be stored or sent over the network, intranet, and Internet. Information resources that store, process, or transmit sensitive-enhanced or sensitive information must have the capability to encrypt information.

9-7.1.1 Minimum Encryption Standards

Synchronous encryption: Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/ retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.

Asynchronous encryption: RSA with a 2048-bit encryption key pair. Elliptic curve algorithms ECDH or ECDSA may be used with key sizes 224-bit or greater. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.

PCI systems also require Transport Layer Security (TLS) protocol version 1.2. New implementations must meet the minimum standard. Legacy systems must have plans for moving to the minimum encryption standard; the associated timeline for this action is based on feasibility (technical capability, business plan for upgrade/retirement, etc.), identification of a published exploit to the implemented encryption algorithm, and associated risk to the Postal Service.

The minimum encryption standard for the Postal Service is the Advanced Encryption Standard (AES) with a 256-bit encryption key. Asynchronous encryption: RSA with a 2048-bit encryption key pair.

9-7.1.2 Required for Transmission and Storage

Information resources storing, processing, or transmitting sensitive-enhanced or sensitive information must implement encryption based on Postal Service encryption and key recovery policies. Encryption must be used for sensitive-enhanced and sensitive information that is transmitted across networks or in transit between [1] an application or batch server and a database server and [2] between workstations and a database server.

Encryption must be used for sensitive-enhanced and sensitive information stored or archived on fixed and removable devices or media (e.g., disks, diskettes, CDs, and USB storage devices).

Encryption must also be used for sensitive-enhanced and sensitive information that is stored off Postal Service premises.

Encryption must be used for non-publicly available electronic information in transit or stored off Postal Service premises.

Encryption must be used for payment card industry (PCI) information throughout the life cycle. Unencrypted primary account numbers (PANs) must not be sent via end user messaging technologies.

9-7.1.3 Recommended for Storage on Postal Service Servers and Mainframes

Where technically feasible, encrypt sensitive-enhanced and sensitive information stored on Postal Service non-removable devices.

9-7.1.4 Required for Workstations and Laptops

Full disk encryption must be installed on all workstations and laptops.

9-7.2 Use of Encryption Products

Encryption products must comply with requirements including, but not limited to, the following:

a. Information resources using encryption must use only algorithms and standard encryption products that are approved by the Postal Service and meet federal information processing standards and industry best practices. Use of locally generated, self-signed digital certificates is prohibited.

b. All encryption products must support functionality of and integrate with security content-filtering applications or make encryption keys available to management. Any use of encryption without such technology must be approved in writing by the CISO.

c. Application owners follow encryption standard operating procedures for their application as documented within their specific EIR deliverables, as required by USPS Handbook AS-805-A (4-4.2 Deliverables, a. Standard operating procedures).

9-7.3 Key Management

Key management is the generation, recording, transcription, distribution, installation, storage, changing, disposition, and control of cryptographic keys. Key management must be rigorous and disciplined because attacks against encryption keys are far more likely to occur and succeed than attacks against encryption algorithms.

9-7.3.1 Protecting Encryption Keys

Encryption keys must be treated as sensitive-enhanced information and access to those keys must be restricted on a need to know basis. The following principles apply to the protection and access of encryption keys:

a. If keying material is generated and stored, the information resource must provide secure key storage that is resistant to compromise through a logical or physical attack.
b. If hardware-based key generation and storage is used, the key must be stored in such a way that it cannot be retrieved in clear text.

9-7.3.2 Recommended Key Management Practices

The best way to mitigate the risk of keys being attacked is to store them in hardware on a secure physical device. Postal Service information resources should adhere to key management procedures and practices that include, but are not limited to, the following:

a. Generate strong keys that meet the Postal Service minimum encryption standards (See 9-7.1.1, Minimum Encryption Standards).
b. Key management should be fully automated and not require manual steps.
c. Generate and store all keys in hardware.
d. Never remove keys from the hardware and never store them in the host's memory.
e. Gain access to the hardware only through a trusted path.

9-7.3.3 Key Management Requirements

Information resources must comply with key management requirements including, but not limited to, the following:

a. If the information resource supports key recovery, then access to the key must be restricted to authorized personnel.
b. The information resource must have the capability to enforce the immediate revocation of user accounts and the associated key(s).
c. Encryption keys must not appear in clear text outside a cryptographic device.
d. Split knowledge keys must be implemented.
e. Dual control of keys must be established.
f. Secure key distribution and storage must be implemented.

g. Unauthorized substitution of keys must be prevented.

h. Keys must be changed periodically, as defined below:

(1) Every year for PCI in-scope applications.

(2) Every 2 years for non-PCI in-scope applications.

(3) Every 3 years for USPS Certificate Authority (CA) Online Subordinate tier Server(s), every 5 years for Offline Policy tier CA server(s), and every 10 years for offline Root tier CA server(s).

(4) Whenever anyone with knowledge of a portion of a key that is NOT stored in a Hardware Security Module (HSM) changes positions, transfers, or for any reason leaves the employ of the Postal Service (e.g., resigns, retires, terminates).

i. Known or suspected compromised keys must be replaced.

j. Old or invalid keys must be revoked.

k. Old keys must be archived and destroyed as applicable.

l. Key custodians must sign a form stating they understand and accept their key-custodian responsibilities.

m. Keys must not be sent in the same email as the encrypted file.

n. Sponsors for nonhuman subscribers (systems, applications, and devices) are responsible for the security of and use of the subscriber's private keys.

o. All subscribers including human and device private keys are not used by more than one entity.

p. Public keys (Digital Certificates) must be changed at least 30-days prior to the digital certificate's expiration date.

9-7.3.4 Public and Private Key Management Agreement

The United States Postal Service (USPS) Cryptographic Keys (aka Private Keys) and Digital Certificates (aka Public Keys); including those provided by third-party vendors intended for use by the USPS, must be used only in accordance with this Public and Private Key Management Agreement, including the following:

a. To use your Cryptographic Key(s) and Digital Certificate(s) exclusively for authorized management of a USPS asset, or authorized USPS business partner asset.

b. To take all necessary precautions to protect your Cryptographic Key(s) and Digital Certificate(s) from loss, disclosure, modification, or unauthorized use, as per this policy derivative; as well as USPS Handbook AS-805C, *Information Security for General Users.*

Every United States Postal employee and contractor shall maintain control of Cryptographic Keys at all times and shall abide by the agreements above.

9-7.4 Cryptographic Hash Function

A cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, hash value, such that an (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded is often called the "message," and the

hash value is sometimes called the message digest. The ideal cryptographic hash function must have the following significant properties:

a. It is easy to compute the hash value for any given message.

b. It is infeasible to generate a message that has a given hash.

c. It is infeasible to modify a message without changing the hash.

d. It is infeasible to find two different messages with the same hash.

The Postal Service cryptographic hash standard is SHA-2 or SHA 256. Older algorithms (e.g., SHA 1) maintained by commercial products and applications used and developed by the Postal Service may continue to be supported since they may be required to validate digital signatures executed in the past and to decrypt objects encrypted in the past using the older algorithms and key sizes. These cases must show acceptable effort of migration to standard algorithms as identified in this policy and receive an exception waiver by the CISO. In addition it is recommended that:

a. A Salt value is always used with your hash. This is especially important if the sensitive data to be protected is short like a, social security number, or a payment card number.

b. Always use a Strong Salt value when creating a credential hash. A Salt is a fixed-length cryptographically-strong random value. Follow these practices to properly implement credential-specific salts:

   (1) Generate a unique salt upon creation of each stored credential (not only per user or system-wide).

   (2) Use cryptographically-strong random data.

   (3) As storage permits, use a 32-byte or 64-byte salt.

c. The Salt value should be protected as any other cryptographic value.

9-7.5 Elimination of Residual Data

The information resource must have the capability to ensure that there is no residual data exposed to unauthorized users.

9-8 Integrity

Integrity is the security property that ensures correct operation of information resources, consistency of data structures, and accuracy of stored information. Information resources must be installed and maintained in a manner that ensures the integrity of the information resources and their data.

Appropriate planning must occur before conducting security-related activities affecting the information resource in order to minimize the impact on the integrity of the information resource and on Postal Service operations (e.g., mission, functions, image, and reputation) and assets. Security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, testing, exercises, and retirement and disposal of hardware and media.

9-8.1 Information Resource Integrity

Information resource integrity ensures that information resources perform their intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Integrity provides assurance that under all conditions the operating hardware and software maintain logical correctness, reliability, and effective protection mechanisms. Acceptable integrity thresholds for processing and control devices in the MPE/MHE private non-routable network address space are defined by Engineering. Information resources must comply with information resource integrity requirements including, but not limited to, the following:

a. Security features designated in approved hardening standards must be invoked.

b. No information resource may undermine the integrity of underlying platforms or supporting infrastructure.

c. The information resource must perform integrity checks for system functions.

d. The information resource must retain the existing security parameters even after a restart or recovery.

e. Backup capability must be provided to restore the information resource to its former state.

f. Boundary checking must be implemented to prevent buffer overflow conditions.

g. The information resource must provide appropriate alert messages before executing potentially damaging commands.

h. The information resource must provide an administrator with the capability of retrieving the date and time associated with any security-related activity and the log-on ID of the user who initiated the activity.

i. The information resource must provide mechanisms to detect duplicate authentic financial transactions.

j. The information resource must monitor the status of its components in real time to ensure that all components are still active and to prevent components from failing without detection.

9-8.2 Data Integrity Requirements

Data integrity is the security property that ensures that data meets a given expectation of quality and has not been exposed to accidental or malicious modification or destruction. All input data must be appropriately validated. Information resources must comply with data integrity requirements including, but not limited to, the following:

a. Information resources must have the capability to ensure that data is not modified, altered, or deleted without authorization in either storage or in transit.

b. Any unauthorized modification of data must yield an auditable security-related event.

c. The information resource must have the capability of identifying the originator of any information before that information is used in any restricted function of the information resource.

d. The information resource must log any attempt by the administrator to authorize any user to bypass the administrator-configured data integrity controls.

e. The information resource must protect data integrity by performing data integrity checks.

f. When data integrity checks fail, the information resource must reject the data.

9-8.3 Application Requirements

Management must be made aware of the accuracy, timeliness, and relevance of the information they use for decision making. Management must be notified if controls which ensure the integrity of information fail or if such controls are suspected of failing.

If information issued or released has been modified in any way, the recipients must be notified about the nature of the modification so that they can determine whether the modifications are significant enough to affect decision making. All incomplete or obsolete information must be suppressed and not distributed to users unless it is accompanied by an explanation which describes the status of the information.

Production data and software must be changed only by authorized people according to established written procedures. Production transactions must be properly authorized prior to updating production records whether these records are computer based or not.

To facilitate tracking and problem resolution, each accountable transaction must be time stamped, identified to person who submitted it, and assigned a unique sequence number or identifier. Line numbering must also be implemented for free-form text messages that deal with important business matters.

Sufficient controls must be implemented to ensure information is free from a significant risk of undetected alteration.

All rejected input transactions must be placed in a suspense file and listed in exception reports until such times as they are successfully resubmitted for processing or otherwise handled. All input transactions that are held in a suspense status pending further investigation must be either resubmitted or otherwise handled within 10 business days of original entry. Input transactions that are corrected for resubmission or that are suspended and later approved resubmission must be subjected to the same validation procedures (e.g., reasonable checks and formal edit checks) that original input transactions receive.

9-8.4 Management Requirements

Internal records must be reviewed semiannually for reasonableness and accuracy. Reasonable checks include ratio analysis and accuracy checks include physical inventories. If records are discovered to be in error, they must be immediately corrected by authorized individuals using standard control procedures.

Important information on which management depends must be compared semiannually with external sources or otherwise cross-validated to verify that it is accurate.

9-8.5 End-User Computing Requirements

End-user computing, including spreadsheets and other user-developed programs, must be documented and regularly reviewed for processing integrity, including their ability to sort, summarize, and report accurately. For important reports, the logic should be reviewed semiannually to verify information is processed completely and accurately. User-developed systems must be secured from unauthorized use. Audit logs must be reviewed daily to detect unauthorized access attempts and take corrective action. To facilitate audit trail requirements, transactions affecting sensitive-enhanced, sensitive, and critical information must be initiated only by receipt of source documents or computerized messages in which the originating individual and system are clearly identified. Proof of non-Postal Service sources can be achieved via digital signatures, message authentication codes (MACs), and encryption. All end-user business-related representations must be truthful at all times.

9-9 Availability

Availability is the security property that ensures information resources are accessible by authorized personnel or information resources when required.

9-9.1 Capacity Planning and Scalability

For all information resources, capacity planning and scalability must be considered for both the information resources and network components, such as routers, firewalls, proxies, and encryption. Whenever technically feasible, consider scalable information resources that require little or no change to the configuration or the application when adding hardware or data storage.

9-9.2 Redundancy

Redundant systems for utilities, communications, mainframes, servers, and firewalls may be recommended where warranted to ensure the availability of critical information resources. The implementation of redundant systems should be based on a cost-benefit analysis and the recovery time objective (RTO). Infrastructure including telecommunication services must be engineered to not have a common point of failure.

9-9.3 Relationship of Criticality, Recovery-Time Objective, and Recovery-Point Objective

9-9.3.1 Criticality

The initial determination of criticality of an information resource is determined during the BIA process. Subsequently, internal and external dependencies must be identified to understand how a given application interfaces with the rest of the Postal Service applications and infrastructure. A system is dependent if it cannot function without the input or connection to the other system or portal. For example, applications which by themselves are not critical may have a higher designation because they provide data to an

application with a higher criticality designation. Any identified dependencies may change the initial criticality designation.

The criticality determination may be further refined by Postal Service management. The criticality designation will be updated in the BIA and EIR by the Business Continuity Group.

9-9.3.2 Recovery-Time Objective

The RTO, which is the maximum allowable downtime for an information resource, is determined for information resource designated as critical. The RTO is the length of time it takes to restore the information resource. The RTO does not indicate how much data will be lost.

The RTO must be commensurate with the level of criticality. If there is a significant mismatch between the RTO and the criticality designation, the RTO and criticality designation must be reviewed. As a general rule the more critical the information resource, the lower the RTO. A lower RTO often requires a larger investment in BCM resources, which, in turn, results in higher costs. The RTO is determined in consultation with the DR service provider as the DR strategy is defined.

9-9.3.3 Recovery-Point Objective

Also at this time, the data currency requirements/recovery point objective (RPO) is determined. The RPO indicates the maximum amount of allowable data loss. It is the point in time (age) to which data must be recovered relative to the time of the disaster. It is the size of the window of opportunity for data loss. The amount of data loss is determined by backup methods and frequency of backup transport offsite.

9-9.4 Assuring Availability

Multiple technologies should be used to minimize the data loss and increase the availability of data for local and alternate site recovery. These technologies must provide for both traditional backup and recovery to meet local requirements in addition to the availability of data at the alternate processing site for disaster recovery. The movement of data for disaster recovery can be moved electronically over high-speed dedicated circuits via hardware data replication, remote tape vaulting, or information resource specific database replication/journaling technologies. The choice of technologies is dependent on the desired RPO and RTO.

9-9.4.1 Data Replication

Selection criteria: The files selected for data replication are determined by the placement of the data on the appropriate storage device that is configured for passive replication. Passive replication refers to a process when the data is changed and stored on the primary device and then the data is replicated to a device at the alternate site.

Frequency: The frequency of data replication should be aligned for minimal data loss and expected RPO for this service.

9-9.4.2 Remote Tape Vaulting

Selection criteria: The files selected for remote tape vaulting are determined by the usage of unique identifier(s) in the file name or specific request to the

IT operations group. The supporting IT operations group needs to be contacted to receive the appropriate unique identifiers or to make specific site requests.

Frequency: The frequency of tape vaulting is dependent on the establish RPO for this service.

Inventory: An inventory of critical files that are remotely vaulted must be maintained. A copy of the inventory must be available at the alternate processing site to support business resumption process.

9-9.4.3 Application Database Replication and Journaling

The application owner who chooses to use a vendor-provided database replication and journaling services for high-availability services must procure the IT-approved product, then fund or perform the necessary configurations and reconfigurations.

9-9.4.4 Alternate Backup Requirements

All information resources not using one of the above technologies must implement secure backups. The information resource must have the capability to check the integrity of data read from a backup file when performing a restore function.

All essential components of an information resource required for continued operations must be backed up. The backup procedures must be documented. The responsible Postal Service manager must define the appropriate backup media and frequency.

Applications determined by the BIA as critical must implement backup and recovery strategies sufficient to meet the RTO and data currency requirements.

9-9.4.4.1 What to Back Up

Backups include, but are not limited to, operating systems, configuration files, general utilities, application software, data, supporting files and tables, scripts, standard operating procedures, specialized equipment, and related documentation.

9-9.4.4.2 When to Back Up

Backup software prior to migrating to test or production and prior to maintenance. Backup software after migrating to production and after maintenance. Backup information updated by batch processing at the successful completion of the update. Backup information updated by real-time processes at a frequency based on the RTO and RPO of the application.

9-9.4.4.3 Backup Schedules

All essential components must be backed up on a schedule that is sufficient to meet the RTO and RPO of the application or information resource as defined by the executive sponsor that controls the essential component and Business Continuance Management. Back-up job failures are properly documented, investigated, and remediated immediately.

9-9.4.4.4 Backup Inventory

An inventory of critical applications backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off site

or in a fireproof container at the facility that hosts the application. An inventory of backup media and materials is recommended for all other information resources.

9-9.4.4.5 Backup Storage Requirements

Backup media containing critical information must be stored in an environmentally controlled and secure location (e.g., a locked cabinet or room with controlled access). Backup media containing sensitive-enhance, sensitive, and non-publicly available information must be labeled as "Restricted Information". Backups must not be stored on the same hardware device as the original information.

9-9.4.4.6 Off-Site Backup Storage Requirements

Critical information stored on mainframes, servers, workstations, and mobile devices must be backed up and must be stored off-site at a location that is not subject to the same threats as the original media. An inventory listing of backup media containing critical information must be maintained at a designated Postal Service facility off site from the primary information location.

Noncritical information stored on mainframes, servers, workstations, and mobile devices must be backed up and stored off site at a location that is not subject to the same threats as the original information. Postal Service information must not be co-mingled with non-Postal Service information.

9-9.4.4.7 Backup Verification

Backup media for critical applications must be verified to ensure that backups are complete and can be read. From time to time, the application and associated backup hardware and software should be tested with the backup media to ensure the application can be successfully restored and used. Verification of backup media is recommended for all other information resources.

Annually review the data backup policies and inspect the actual backup practices of third party providers.

9-9.4.4.8 Backup Disposal

All unneeded electronic backup media or hardware containing sensitive-enhanced or sensitive electronic media must be erased using a method that complies with the most current Postal Service policy and processes on the disposal of sensitive-enhanced and sensitive media. (See 3-5.8, Disposal and Destruction of Information and Media.)

9-9.5 Information Resource Recovery and Reconstitution

Critical information resources, including infrastructure and applications, must have the ability to be recovered and reconstituted to their original state following a disruption, failure, or disaster. This means all system parameters (either default or established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application software is reinstalled, information from the most recent backups is available, and the entire

configuration has been fully and successfully tested at an alternate site. Authorization to request backup data is limited and restricted to approved Postal Service personnel.

Contingency plans must be developed and tested for critical infrastructure and telecommunication service providers and include recovery and reconstitution of critical applications. The EIR must be updated to identify which applications require the development and testing of continuity plans.

The frequency for testing business continuity plans for critical-moderate and critical-high applications is defined in 12-2. Business continuity plans for critical-high applications must be tested at an offsite location using only software, data, scripts, and procedures stored at the offsite backup location. The business continuity plans must be updated annually based on the lessons learned from testing.

9-9.6 High Availability

High availability should be implemented where warranted, based on a cost benefit analysis and RTO. Resources or processes that may be deployed to ensure high availability include, but are not limited to, the following: a. Fault-tolerant information resources.

b. Redundant hard drives (e.g., randomly accessed independent disk [RAID] array), systems, and servers.

c. Uninterruptible power supplies (UPS), power conditioning systems, and backup generators.

d. Off-site vaulting of application transactions.

e. Disk mirroring of applications at site not subject to the same threats. Disk mirroring does not negate the need for backups. Mirroring only ensures both instances are the same (i.e., both instances can be blank or incorrect).

f. Hot-swappable components.

g. Secondary storage devices.

h. Continuous monitoring.

i. Automated fail-over and fail-back systems.

9-10 Security Administration

Security administration includes management constraints, operational procedures, and supplemental controls established to protect information resources. Sensitive-enhanced, sensitive, and critical information resources must implement logical access security.

9-10.1 Security Administration Requirements

Security administration functions that must be implemented for Postal Service information resources include, but are not limited to, the following:

a. Activating protective features (e.g., the login feature).

b. Displaying users logged on.

c. Creating, retrieving, updating, or deleting all security–related attributes of users, interfaces, and software and data elements.

d. Overriding or altering vendor-provided security defaults.

e. Configuring security-relevant options.

f. Configuring the display of security-related events.

g. Recording and archiving the information resource configurations.

h. Monitoring suspected activities related to a potential information security incident.

i. Detecting information security incidents immediately, isolating and investigating the problem, and recovering securely from the incident.

j. Provide a level of access and documentation necessary to perform comprehensive security assessments of an information system, application, or hardware when performing the following functions:

1. Incident Response
2. Investigations of Cyber Risk
3. Penetration Testing

9-10.2 Security Administration Documentation Requirements

Security administrative requirements must be appropriately documented. These security administration documentation requirements include, but are not limited to, the following:

a. Cautions about functions and privileges that must be controlled when running a secure facility.

b. Administrator functions related to security, including adding or deleting users, changing user security characteristics, generating keying material, and revoking user-related security parameters.

c. Standards on consistent and effective use of security features, including their interaction and how to generate a new security configuration.

d. Standards for retaining accountability tracking information for an administrator-specified period of time.

e. Procedures necessary to start the information resource in a secure manner.

f. Procedures to resume secure operation after termination of information resource processes.

9-11 Audit Logging

All information resources must implement system-level audit logging. Audit logs include operating system logs, application system logs, database system logs, event logs, error logs, and Web logs. CISO must have access to all security-related audit logs. Information resources must support audit log capabilities including, but not limited to, independently and selectively monitoring (in real time) the following:

a. The actions of any user currently logged on and automatic lockout of that user if necessary.
b. The activities at a specified terminal, port, or network address and automatic lockout of that input device if necessary.

9-11.1 Audit Logging Functionality Requirements

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred. Information resources must implement audit logging functions including, but not limited to, the following:

a. Providing adequate information for establishing audit trails relating to information security incidents (as part of forensics analysis) and user activity.
b. Where feasible, consolidate audit records from all sources for automated analysis, alerting, and archiving in support of compliance, accountability, and security.
c. Supporting administrator-selectable alerts for specified security- related events.
d. Recording the log-on ID or user ID accountable for the event.
e. Maintaining the confidentiality of authenticators (e.g., passwords) by excluding them from being recorded.
f. Maintaining the confidentiality of personally identifiable information (PII) and debit/cardholder data.
g. Protecting audit logs as sensitive information.
h. Protecting audit log control mechanisms from modification, deletion, or disabling of the function.
i. Restricting access to authorized users.
j. Generating real-time alarms indicating immediate attention is required for operational problems (e.g., running out of storage space) and audit log malfunctions. USPS Authorizing Official(s) (AOs) ensure that reports on information security operations status and incident reporting are provided to the policy authority as required by this policy.
k. Providing authorized individuals with access to enable retrieval, printing, and archiving (copying to long-term storage devices) of audit log contents.
l. Providing administrators with audit analysis tools to selectively retrieve records from the audit log to produce reports.
m. Sanitizing audit log storage locations and media prior to reuse.

9-11.2 Audit Log Events

The logging of the following events must be considered for information resources:

a. All sessions established.

b. All authentication attempts (i.e., valid/authorized and invalid/ unauthorized) to access information resources.

c. Action of individuals with root or elevated privileges (e.g., system and database administrators).

d. Creation or changes in user or information resource security accounts, profiles, ACLs, privileges, and attributes.

e. Creation and deletion of system level objects.

f. Use of privileged accounts.

g. Shutdowns, restarts, and backups.

h. Installation and updates of software.

i. Access to audit logs.

j. Changes to log configurations.

k. User Access to Cardholder data.

For the specific security events to capture for a particular platform, see the appropriate hardening standards.

9-11.3 Audit-Log Contents

The information resource must record event information including, but not limited to, the following when available:

a. Date and time of the event.

b. Log-on ID and MAC or IP address of the event initiator.

c. Event type and success or failure of the event if applicable.

d. Identification of information resources accessed.

e. Source host name and IP address generating the log event.

f. Destination host name and IP address generating the log event.

g. Transaction code or process ID.

9-11.4 Audit-Log Protection

Secure audit logs so they cannot be altered by:

a. Labeling audit logs as "RESTRICTED INFORMATION."

b. Limiting the viewing of logs to those with job-related need (e.g., need to know and least privilege).

c. Protecting audit log files from unauthorized access, modifications, and destruction.

d. Immediately backing up audit log files to a centralized server or media that is difficult to alter.

e. Storing a backup copy of audit logs off site.

f. Using file integrity monitoring and change detection software on logs to ensure existing log data cannot be changed without generating alerts.

9-11.5 Audit-Log Reviews

System administrators and database administrators must review audit logs regularly for potential security incidents and security breaches and maintain a record of the review. System administrators and database administrators must review audit logs regularly for potential security incidents and security breaches and maintain a record of the review. For PCI in-scope applications, audit logs must be reviewed daily. Any suspicious activity must be reported to management and CyberSafe, investigated, documented, and resolved immediately. See Audit-Log Events for details regarding the events that should be captured for each platform.

9-11.6 Audit-Log Retention

Audit logs, whether in electronic or nonelectronic format, must be retained in accordance with a legal hold (e.g., FOIA request, subpoena, law enforcement actions), or as directed by the Postal Service Records Office (see Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management)* and then destroyed in accordance with Postal Service policy.

For PCI in-scope applications, audit logs must be retained for at least one year with a minimum of 3 months immediately available for analysis; (i.e., processes must be in place to restore at least the last three months of logs for immediate analysis).

Industry audit log retention best practice is 2 years online and federal government audit log retention best practice is 18 months online.

10 Hardware and Software Security

10-1 Policy

Postal Service policy is to manage the procurement, configuration, operations, and maintenance of information resource hardware and software, whether located on Postal Service or non-Postal Service premises, in a manner that ensures information security. Hardware and software security must be implemented and maintained with the appropriate level of technical and administrative controls to protect the Postal Service technology and operations infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction. Chapter 10 addresses the following:

a. Hardware security.
b. Software and applications security.
c. General policies for hardware and software.
d. Configuration and change management.
e. Protection against viruses and malicious code.
f. Operating system, database management system, and application audit log requirements.

10-2 Hardware Security

Hardware security must be implemented based on Postal Service published standards on all computer hardware including, but not limited to, the following:

a. Mainframes.
b. Network devices.
c. Servers.
d. Workstations.
e. Mobile computing devices.

10-2.1 Mainframes

Appropriate security controls must be enabled. For mainframe implementation of this security policy, contact the manager, Host Computing Services.

10-2.2 Network Devices

Appropriate security controls must be enabled on all network devices, including servers, routers, hubs, and switches (see 11-3, Protecting the Network Infrastructure).

10-2.3 Servers

A server is a host that provides one or more services for other hosts over a network as a primary function. Servers include outward-facing publicly accessible servers (such as Web and email services); inward-facing servers (such as storage-based information resources like file servers, Network Attached Storage [NAS] servers, Storage Area Network [SAN] servers, database servers, application servers, directory servers, domain name servers); highly specialized servers like security infrastructure devices (such as firewalls and intrusion detection systems); and virtual servers.

Postal Service servers must be protected commensurate with the level of sensitivity and criticality of the information and business function. Server installation and deployment must comply with standard configuration and deployment standards unique to the individual server platform. Implement only one primary function per server [e.g., a Web server, database server, and domain name server (DNS) should be implemented on separate servers).

The following security activities are required to securely administer Postal Service servers:

a. Harden server and configure operating system to address security.

b. Identify vulnerabilities and install additional mitigating controls as required.

c. Implement Postal Service change control procedures.

   (1) Apply and test non-critical patches in a timely manner.

   (2) Implement critical security patches according to Postal Service standards.

   (3) Implement a management process over script automation that includes documentation and inventory of automated scripts.

d. Control automated time synchronization (also see 11-2, Network Infrastructure).

   (1) Implement Network Time Protocol (NTP) or similar technology for time synchronization.

   (2) Designate specific external hosts (i.e., industry-accepted time sources) from which the designated Postal Service time servers will accept NTP time updates.

   (3) Implement controls to prevent internal servers from receiving time signals from any source other than the Postal Service-designated internal NTP servers.

   (4) Restrict access to time data to individuals with a need to access time data.

   (5) Log, monitor, and review all changes to time settings.

e. Determine the best authentication credentials for each operating environment.

f. Implement access control.

   (1) Implement the Postal Service access control policy.

(2) Monitor password aging. Passwords associated with devices that do not have the ability to monitor password aging for local accounts must be submitted for approval as non-expiring passwords.

(3) Conduct semiannual review of all access.

g. Only accept connections from remote clients configured to Postal Service standards.

h. Implement Postal Service standards for audit logging (see 9-11, Audit Logging).

(1) Analyze log files on a frequent basis.

(2) Retain log files according to the applicable system of record.

i. With the application owner determine if server is production or non- production and the server's criticality.

j. Back up critical information and all server software frequently and send backups offsite in accordance with Postal Service processes.

k. Develop appropriate contingency plans and procedures.

l. Establish and follow procedures for recovering from compromise.

m. Implement the following security principles:

(1) Fail safe – fail in a secure manner; (i.e., default to no access).

(2) Separation of privilege – provide a much granularity as possible.

(3) Least privilege – grant minimum rights to perform a task.

(4) Psychological acceptability – implement sensible options that are user acceptable and effective.

(5) Least common mechanism – grant a function to a single process or service.

(6) Defense in depth – implement layered security mechanisms.

(7) Work factor – the amount of work necessary for an attacker to break the system or network should exceed the value of the data or resource availability that the attacker would gain.

(8) Compromise recording – logs provide sufficient evidence if a compromise does occur.

n. Test security controls periodically.

o. Conduct vulnerability scans and penetration tests.

Configuration standards for servers in the mail processing and mail handling equipment (MPE/MHE) non-routable address space environment are defined by Engineering.

10-2.3.1 Hardening Servers

All information resources must be implemented on servers hardened to Postal Service standards. Hardening standards are based on CIS sources and vendor recommendations which must be implemented specific to each platform. These standards must delineate restricted and prohibited functions, port, protocols, and services and include details on how to configure systems with approved security parameter settings.

Server hardening standards must require the removal of unnecessary functionality such as drivers, scripts, subsystems, and file systems.

Hardening standards must be updated as new vulnerabilities are uncovered and updates are available. Hardening standards must be reviewed and updated at least annually. This requirement includes hardening standards for mainframes, servers, networks, and firewalls.

Operating system and database software configurations, including services, protocols and functionality, must be reviewed on a periodic basis commensurate with the level of sensitivity and criticality of the information and business function. Operating system software configuration reviews are performed on a semi-annual basis for UNIX. Unnecessary services and protocols must be disabled. All unnecessary functionality such as scripts, drivers, features, subsystems, and file systems must be removed. Vendor supplied default passwords must be removed and common parameters must be set to prevent misuse or compromise.

Servers must not be deployed to a production environment prior to hardening. Servers must be updated when the server hardening standards are updated for that platform.

Note: The manager, Corporate Information Security Office (CISO) Information Systems Security (ISS), is responsible for the update and distribution of server hardening standards

10-2.3.2 Web Servers

All Postal Service Web servers, regardless of location, must use approved hardware and software with standard configurations to reduce likelihood of loss or compromise due to exploitation of configuration vulnerabilities. For Web or Internet projects under the direct control of the Postal Service, the development and testing must be conducted on specifically designated development Web servers. Web servers must not be implemented on individual workstations without prior written approval by the manager, CISO ISS.

10-2.3.3 Database Servers

Database servers must use security controls appropriate for the level of sensitivity and criticality of the information they contain. Database servers must be separate from other servers, including Web and application servers (see 10-2.3.4, Combined Web and Database Servers, for an exception).

Database servers located inside Postal Service firewalls must not be directly accessible from Web servers or other systems located outside firewalls. All database servers must be approved by the Network Change Review Board (NCRB) prior to being deployed to the demilitarized zones.

Database servers must not be deployed to a production environment before hardening.

10-2.3.4 Combined Web and Database Servers

A Web server and database server may be placed on the same host if all the following requirements are met:

a. Application is not sensitive-enhanced, sensitive, or critical.

b. Application is not Internet accessible.

c. Application is not on the DMZ.

d. Application is not enclaved with sensitive-enhanced, sensitive, or critical applications.

e. Application is operationally standalone, that is, does not interact with other database servers.

f. Host meets Postal Service server hardening standards.

10-2.4 Workstations and Mobile Computing Devices

All workstations and mobile computing devices including desktops, laptop computers, notebook computers, and tablet computers must have appropriate security controls. Workstation and mobile computing device installation and deployment must comply with standard configuration and deployment standards unique to that platform. All personnel are responsible for protecting the information resources at their individual work location and abiding by all information security policies and procedures that apply to their individual environment.

All Postal Service workstations and laptops must have an approved personal firewall installed and personnel must connect to the Postal Service intranet at least once per week to receive the latest software patches, antivirus pattern recognition files, and personal firewall patterns. Appropriate configuration of the workstations and laptops to receive these patches and pattern updates is required.

All workstations processing PCI information and all laptop computers, notebook computers and tablets must implement full disk encryption. In addition, sensitive-enhanced, sensitive, and critical information on other mobile computing devices must be protected (e.g., encrypted) when leaving a secure environment. All media subject to loss or removal from Postal Services premises must be encrypted. Only procure Postal Service approved devices from approved sources. Only use USB flash drives and removable media that are encrypted. Back up critical information frequently and send backups offsite in accordance with Postal Service procedures. Critical information must not be backed up on the same device as the primary information.

10-2.4.1 Physical Security

All Postal Service workstations and mobile computing devices must be protected, at a minimum, by secure physical access to the facility or room. Other physical security controls may include, but are not limited to: unique platform identification (inventory control), identification card reader, screen

protector or positioning screen to restrict viewing from passersby, lockable keyboard, physical lock, and desk-fastening security equipment.

10-2.4.2 Password-Protected or Token-Protected Screen Saver

Where feasible, all workstations and mobile computing devices must be configured prior to deployment to use password-protected or token protected screen savers. After a period with no activity, password-protected screen savers will blank the screen; a password or token is then required to resume work. Users must protect the screen saver password or token just as they protect all other system passwords.

10-2.5 Mobile Computing Devices

Mobile computing information resources must be protected against damage, unauthorized access, and theft. All personnel who use or have custody of mobile computing devices, such as, handheld computers, smart phones devices, wireless telephones, and removable storage media devices, are responsible for their safekeeping and the protection of any sensitive-enhanced, sensitive, and critical information stored on them.

All laptop and notebook computers must implement hard disk encryption. In addition, sensitive-enhanced and sensitive information on other portable devices must be protected (e.g., encrypted) when leaving a secure environment. All media subject to loss or removal from Postal Services premises must be encrypted. Only procure Postal Service approved devices from approved sources. Only use USB flash drives that are capable of encryption.

All mobile computing devices must be managed by a Mobile Device Management (MDM) solution. The MDM solution must be vetted and approved by CISO.

Data on all mobile devices must be systematically eradicated before transferring to another individual or disposal.

10-2.6 Bring Your Own Device

Personnel must not load Postal Service information on their own computing device or connect their own computing device to the Postal Service network.

10-2.7 Hardware Asset Inventory

A comprehensive, accurate, and up-to-date Hardware Asset Inventory must be maintained and must include all technology assets known to the organization, with the potential to store or process information. This inventory must include all hardware assets, whether currently connected to the organization's network or not. The inventory must be capable of being dynamically updated using active or passive network discovery tools and other network configuration management tools such as Dynamic Host Configuration Protocol (DHCP).

The Hardware Asset Inventory must contain detailed identifying and technical information about each hardware asset in the inventory. This information must include, at the least, network address, hardware address, machine name, data asset owner, owner's department, and asset type. In addition, the

inventory must denote whether the asset has been approved for connection to the network.

10-3.1

10-2.7.1 Active Hardware Discovery

An active discovery tool must be used on a regular basis to identify all devices currently connected to the organization's network. The discovery tool must have the ability to actively scan the entire network upon demand. The active tool should update the hardware asset inventory with the results of this discovery, such that the inventory can report on those devices currently attached to the network.

10-2.7.2 Passive Hardware Discovery

A passive discovery tool must be used to identify and log all devices at the moment the device connects, or attempts to connect, to the network. The hardware asset inventory should be updated with the results of the passive logging, such that the inventory can report on the status of hardware assets upon their initial connection to the network.

10-2.7.3 DHCP Logging

Dynamic Host Configuration Protocol (DHCP) must be used to assign dynamic IP addresses and the assignment of these addresses must be logged and used to update the hardware asset inventory.

10-2.7.4 Hardware Asset Removal

Unauthorized hardware assets, as denoted in the hardware asset inventory, must be actively removed from the network or quarantined by assignment to a specific network segment. In addition, the asset inventory must be updated to reflect the exclusion or quarantining of the asset.

10-2.7.5 Network Access Control

Network Access Control (NAC) is the technique for network management and security that enforces policy, compliance and management of access control to a network. The Network Access Control (NAC) Process supports the Handbook (HBK) AS-805, Information Security Policy for Information Security Services.

Phase 1 – Authorize Hardware and Software into TIPA
The introduction of new devices and software into the USPS® environment must go through the appropriate activities for authorization. The authorization of hardware and software assets occurs in the Technology Initiative Prioritization Assessment (TIPA) Process. The TIPA Process evaluates all hardware and software assets seeking access to the USPS® networking environment and either approves or denies such requests.

Phase 2 – Authenticate Hardware and Software
After TIPA approval, Hardware and Software assets will be authenticated by undergoing the following:

a. Software will be verified through ITK, authorized application and code signing. Hardware will undergo port-level access control by utilizing the 802.1x authentication process to ensure a digital certificate signed by a USPS®

Certificate Authority (CA) is present on both the device and the authentication server.

b. Realizing that all devices don't support 802.1x authentication, security tools will interrogate all devices, pulling hardware and software attributes from the device to establish a unique fingerprint.
c. Upon TIPA approval, required asset data information will be supplied to CMDB.
d. Fingerprints will also be used to confirm that authorized devices adhere to USPS® compliance guidelines and apply the appropriate Network Access Control (NAC).

Phase 3 – Health Check
A health check is performed to provide ongoing monitoring to confirm assets are compliant as follows:

a. Monitor assets to confirm required capabilities are current and operational (i.e. end point protection, patching levels, hotfixes, etc.)
b. Perform Health Check on Hardware and Software Assets to identify end of life status for devices requesting access to the network.

Phase 4 – Security Monitoring of Assets
Once a device is authorized through an authentication process, the device shall be granted access to the network and will continue to be measured for compliance to USPS® Policy. Results will be monitored by the USPS® Cyber Security Operations Center (CSOC) Team as per the Cybersecurity Incident Response Plan (CSIRP).

CSOC enacts a multi-pronged approach to continuously monitor for possible cyber threats to the Postal network. The CSOC monitors the USPS® networking environment for all assets attempting connectivity and have the authority to block or quarantine any asset that does not comply with USPS® Policy.

Cybersecurity Compliance - To support the NAC Process, the CIS Critical Security Controls continue to be addressed to ensure only authorized computing devices and software are given access to the USPS® networking environment. The cybersecurity controls ensure all unauthorized computing devices are found and prevented from gaining access. This also ensures all unauthorized software is found and prevented from installation or execution.

Contact Information - The Information Security Executive Council provides oversight for the implementation and management of the Network Access Control (NAC) MI document. The Information Security Executive Council consists of appropriate Postal Service representatives and serves as a steering committee advising the CISO and promulgating information security throughout the Postal Service.

For questions about the Information Technology Asset Access Control Management Instructions, please contact the Corporate Information Security Office (CISO).

The following diagram illustrates the phases and activities for authorizing, authenticating and monitoring computing devices and software requesting or requiring access to the USPS® networking environment.

Approval Phase	Authentication Phase	Health Check Phase	Security Monitor Phase

Hardware and Software	Hardware	Hardware	Hardware and Software
• Technology Initiative Prioritization Assessment (TIPA) Process • Approve or Deny • Register in ITK or CMDB	802.1 x Authentication (Port Level Access Control) Fingerprinting Configuration Management Database (CMDB) Assets	Fingerprint – OS, make, model	• CSOC authority to identify incidents • Apply appropriate controls, e.g., restrict, deny or quarantine Anything failing could be quarantined
	Software	Software	
	• IT (Information Toolkit) • Authorized Application • Code Signing • Fingerprinting • Configuration Management Database (CMDB) Assets	• Ensure protection tools are up-to-date and in compliance, e.g., SEP, Tanium, SCCM, Cisco AnyConnect Anything failing could be quarantined	

10-2.7.6 Client Certificate Authentication

The organization must use client x.509 digital certificates to authenticate hardware assets connecting to the organization's trusted network.

10-3 Software and Applications Security

Security attributes and capabilities must be considered in the purchase/ acquisition or development of all Postal Service software. The collection of features of the operating system, application, database management system, and utility software must be complementary and enhance the security of the system.

10-3.1 Software Safeguards

Software configuration and installation must include only the features, services, and functions necessary to perform the required business activities.

Controls must include, but are not limited to, the following:

a. Activating or enabling all safeguards embedded in computer software to restrict access to authorized users, maintain system performance, and to monitor for suspicious activity.

b. Documenting information security settings in the security plan and updating the settings during the software lifecycle to continuously provide required level of protection.

c. Disabling or removing all features and files that have no demonstrable purpose.

d. Disabling or removing default privileged log-on IDs, changing all default passwords, and removing guest accounts.

e. Removing test data.

f. Prohibiting use of administrative and root accounts for running production applications.

g. Limiting access to the specific files required.

h. Restricting access to systems software utilities to a limited number of authorized users on the basis of need-to-know.

i. Syncing privileges with various application roles.

j. Using HTTPS to secure the credentials on Web login pages.

k. Using Postal Service certificates on internal HTTPS Web pages.

l. Including the Postal Service logo on the initial application Web page.

m. Using only Postal Service standard encryption. If an encryption solution is not compliant with the current Postal Service standard, then either an EAC review or an exception must be requested.

n. Disabling directory enumeration on the servers.

o. Reviewing software for unauthorized products quarterly.

For PCI in scope applications, the following controls must also be included:

a. Prohibiting the caching to workstations the following file types: doc, txt, pdf, html, htm, tif, gif, jpeg, jpg, xls, etc.

b. Prohibiting the ability to enter an application Web URL and pull data from the application without authentication.

c. Implementing only one primary function per server.

10-3.2 Complying With Copyright and Licensing

All software used on Postal Service information resources must be purchased in accordance with Postal Service policies and procedures and be licensed and registered in the name of the Postal Service. All personnel must abide by software copyright laws and must not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

10-3.3 Secure-Transaction Compliance

10-3.3.1 Financial Requirements

Financial requirements must be implemented when processing e-Commerce financial transactions (Note: these requirements are set by the payment card industry).

10-3.3.2 Medical Information Requirements

Appropriate security requirements must be implemented when processing health or medical information.

10-3.4 Version Control

All software that can be modified must be managed through the authorized Postal Service change control and management process (see 10-5, Configuration and Change Management). Software containing modifications, such as exits and supervisor calls, must be documented detailing the extent of the modifications. The modifications must be fully reviewed, tested, documented, and installed in a controlled environment to avert possible adverse effects on the security of the production environment.

10-3.4.1 Updating Software

Only authorized personnel may perform updates to the production application programs or operating system libraries/directories.

Individual access privileges must be approved by appropriate management officials.

After the system is changed, the security controls must be checked to ensure the security features are still functioning properly. Periodically (at least annually) the security controls must be tested to ensure the information security controls are functioning as designed and documented.

Significant change will cause the reinitiation of the C&A process. The criteria for recertification are defined in Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process,* 6-2.

10-3.4.2 Distributing Software

Controls must be in place to regulate and manage the distribution of Postal Service system-wide production applications to field sites. These controls must ensure that the correct version is installed on all nodes and that the code cannot be modified on the field computer systems.

10-3.4.3 Prohibited Software

Do not install software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software.

Software no longer on the infrastructure toolkit (ITK) must be removed from the Postal Computing Environment (PCE). Use of unsupported software must be approved by IT management and maintained by IT or one of IT's contractors, or removed from the PCE. Direct all requests for software not on the ITK to the Enterprise Architecture Committee (EAC) (see 10-4.2, *Acquiring Hardware and Software).*

10-3.4.4 Unapproved Software

Unapproved software is removed by the IT staff. The Postal Service must ensure that unauthorized software discovered during software inventory scans is deinstalled or if the software is unknown or inaccurately noted as unauthorized, then the software inventory must be updated accordingly.

10-3.4.5 Source Code

Acquired mission critical software will include source code where feasible. A written consent of the authorizing official is required for exceptions to this source code requirement. The acquisition and use of binary or machine executable code without the source code must be accompanied with a vendor warranty.

10-3.5 Operating Systems

All Postal Service information resources must use approved vendor-supported operating systems, including all approved updates and patches. Operating systems must have controls in place to prevent a compromise of the integrity of the computer operating system environment and must be configured to comply with operating system security requirements specified by Postal Service policies. All information resources using vendor-unsupported operating systems must maintain risk acceptance documentation as specified by 10-4: General Policies for Hardware and Software.

10-3.6 Application Software

Postal Service information resources must use only approved application software. Application software must be compatible with installed security software. Security activities for application software must be incorporated in the applicable life-cycle process during development. Application software developed in house or outsourced is subject to the C&A process.

10-3.7 Database Management Systems

All Postal Service information resources must use Postal Service-approved database management systems (DBMSs) that have been configured to comply with Postal Service security policies including:

a. Implement role-based access.

b. Authenticate all access by information resources, administrators, and users.

c. Prohibit direct SQL queries to the database.

d. Prohibit database servers located inside Postal Service firewalls from being directly accessible from Web servers or other information resources outside those firewalls.

10-3.7.1 DBMS Activity Journals

Each production DBMS must have a journal file to protect against accidental destruction of data or interruption in service. Journal files must be backed up as specified in the DBMS or the applicable business continuity plan.

10-3.7.2 DBMS Security Features and Views

All database tables must utilize the security features of the DBMS or the platform access control software (e.g., mainframe) to preserve the integrity of the database. Views and discretionary access controls must be used to protect sensitive-enhanced, sensitive, or critical information and enforce need to know.

10-3.8 Web-Based PCI Applications

Web-based PCI applications must deploy an application firewall in front of the Web site or hire a qualified third party to evaluate the Web-facing applications in accordance with the current PCI DSS.

10-3.9 COTS Software

Commercial-off-the-shelf (COTS) software must be purchased from a Postal Service-approved source. The EAC approves COTS software for use within the Postal computing environment. Requests for unapproved COTS software must be submitted to the EAC for review and approval.

Computer software purchased for the Postal Service must be registered to the Postal Service. COTS software used within the MPE/MHE non-routable address space environment is approved by Engineering.

COTS software used to process payment card information must be in certified by a Payment Application Qualified Security Assessor. The certification status of the COTS software must be checked prior to acquisition and before major new software releases are installed.

10-3.9.1 COTS Software Security Evaluation and Vulnerability Assessment

A COTS software security evaluation and vulnerability assessment must be performed for all proposed additions to the Postal computing environment. It is recommended that the COTS vulnerability assessment be updated for COTS software associated with sensitive-enhanced, sensitive, and critical information resources when first installed and for every version update.

10-3.9.2 COTS Independent Code Review

COTS applications that contain custom programming or scripts may be subject to an independent code review. An independent code review examines the custom source code and documentation to verify compliance with software design documentation, programming standards and to ensure the absence of malicious code. COTS custom programming or scripts may require a code review. COTS modification without authorization by the EAC is prohibited. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for the criteria for conducting an independent security code review.)

10-3.10 Browser Software

10-3.10.1 Approved Browser Software

Workstations and applicable mobile computing devices should use Postal Service-approved standard browser software. Web applications developed for Postal Service use must be compatible with Postal Service-approved

standard browser software. The software must support encryption and comply with the privacy and cookie policies found at *www.usps.com*.

10-3.10.2 Cookies

Cookies are defined as:

a. Session cookie is a small piece of textual information that a server places temporarily on your browser during the time your browser is open. The cookies are erased once you close all browsers.

b. Persistent cookie is a small piece of text stored on a computer's hard drive for a defined period of time, after which the cookie is erased. The Postal Service must not collect or link to personal information through persistent cookies without customer's express consent.

Use of cookies on externally facing websites is detailed in Postmaster General Letter on Cookie Usage dated 23 January 2008 and is restricted to the following:

a. Session cookies may be used to support transactions, logging on and off the site, and computing postage.

b. Persistent cookies are allowed for the following limited purposes:

(1) To gather non-personal usage statistics such as how many new, repeat, and total visitors use our Web site.

(2) To support advertisements or promotions.

(3) To recognize customers or their information on a return visit, but only if they have expressly told us they want to be so recognized.

c. Further detailed information on allowable use of cookies is contained in the USPS privacy policy at *http://about.usps.com/who-we-are/ privacy-policy/welcome.htm*

10-3.11 Third-Party Software

Third-party software is defined as follows:

a. Software developed for the Postal Service by a vendor, contractor, supplier, or other third party.

b. Other limited-distribution custom-built applications.

c. COTS software that has been modified with custom programming scripts or languages.

10-3.11.1 Ownership

Third-party software developed under contract or funded by the Postal Service must be considered the property of the Postal Service unless otherwise stated in the contract.

10-3.11.2 Licensing and Escrow of Custom-Built Applications

Third-party software not owned by the Postal Service but considered a required component of an information resource used in an essential business activity must be licensed to the Postal Service. The vendor of this software must escrow the source code for each new version submitted to the Postal Service. This escrow requirement must be included in the contract's Statement of Work.

10-3.11.3 Assurance of Integrity

A written integrity statement must be provided with significant third-party software that provides assurances that the software does not contain undocumented features or hidden mechanisms that could be used to compromise the software or operating system security.

10-4 General Policies for Hardware and Software

10-4.1 Securing the Postal Service Computing Infrastructure

The Postal Service computing infrastructure must be protected through the implementation of information security standards, processes, and procedures.

Note: The manager, CISO ISS, is responsible for developing and maintaining an Enterprise Information Security Architecture and coordinating a secure Postal Service computing infrastructure by setting standards, and developing and/or approving the security processes and procedures.

10-4.2 Acquiring Hardware and Software

All hardware and software must be approved and purchased from approved Postal Service sources. Hardware and software not listed on the Infrastructure Toolkit (ITK) must be approved by the Enterprise Architecture Committee (EAC).

Only encrypted USB flash drives are approved for purchase. Encrypted USB flash drives, available from approved Postal sources, are the only USB drives authorized for use in the Postal environment.

All workstations and laptops must be capable of full disk encryption.

All removable electronic devices including laptops, notebooks, tablets, smartphones, external hard drives, and removable media must be encrypted.

10-4.3 Using Approved Hardware and Software

10-4.3.1 General Acquisition Policy

All Postal Service information resources must use only hardware and software purchased from approved Postal Service sources. All Postal Service information resources must use only software listed on the ITK.

Software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software must not be installed. Personnel wishing to use information resources not on the ITK must obtain approval from the EAC.

Engineering must approve hardware and software used within the Engineering private MPE/MHE network.

10-4.3.2 Shareware and Freeware

In addition to approval by the EAC, shareware and freeware must have a formal code review performed and must be scanned for viruses and malicious code and evaluated for security defects prior to use on any Postal Service information resource. Postal Service approved instances of share and freeware must be code signed, appropriately licensed, inventoried, and stored in a Postal Service repository for all future usages.

10-4.3.3 Teleworking

Where Postal Service non-public information is processed via teleworking, organizations should issue teleworkers a Postal Service ACE laptop.

10-4.4 Testing of Hardware and Software

Thorough testing of all new or modified hardware and software is required to ensure that there is no adverse effect on the security of Postal Service information resources.

10-4.5 Tracking Hardware and Software Vulnerabilities

Designated personnel in Customer Care Operations, Host Computing Services, Information Systems Security, and Engineering must be on hardware and software vendor advisory mailing lists and other forums appropriate to the information resources under their control. All vulnerability advisories involving hardware and software in use within the Postal Service computing environment must be documented and tracked.

10-4.6 Scanning Hardware and Software for Vulnerabilities

Scanning tools must have the ability to update the list of vulnerabilities to be scanned and must be scanned on a regular basis. The scanning procedure must ensure adequate scan coverage and update the list of vulnerabilities. Hardware platforms and software packages must be scanned on a regular basis. The scanning procedure must ensure adequate scan coverage and update the list of vulnerabilities.

For in-scope PCI externally facing applications, vulnerability scans must be performed quarterly by a PCI Approved Scanning Vendor (ASV). For in-scope PCI internal applications, vulnerability scans must be performed quarterly by a qualified resource.

10-4.7 Maintaining Inventories

10-4.7.1 Corporate Software Inventory

An enterprise-wide software inventory must be maintained. The enterprise-wide software inventory management process must ensure accountability and appropriate documentation. An accurate and up-to-date software inventory must be maintained that includes all authorized software that is required in the enterprise for any business purpose on any business system. The software inventory must track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.

10-4.7.2 Individual Information Resource Inventories

All personnel are responsible for ensuring accurate inventories are maintained of Postal Service information resources assigned to them including hardware, non-ACE software, firmware, and documentation. The inventory management process must ensure accountability and must include current copies of hardware and non-ACE software maintenance agreements, licenses, purchase orders, and serial numbers. The inventory must indicate the individual authorized to use the information resource. The category supports granting access to auditors or other authorized personnel. The business system owner (VP or Mgrs.) grants access to auditors or other authorized personnel and the FSC (Functional System Coordinator) reviews and provides access. Information resources supporting PCI are labeled with information that can be correlated to the application purpose, owner contact information, and the personnel authorized to use the information resource.

Payment cardholder media must be inventoried and the inventory reconciled semiannually.

10-4.7.3 Vendor Software Support

The Postal Service must ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Software inventory should be continually monitored and updated in order to reflect any changes to a vendor's support for authorized software. Unsupported software should be marked as unauthorized, as the Postal Service should only authorize and install software which is currently supported by the vendor and which receives necessary security updates.

10-4.7.4 Dynamic Software Discovery

The Postal Service must use dynamic software inventory tools to automate the discovery and documentation of all software currently installed on all business systems.

The Postal Service should utilize a tool (such as ForeScout) that can enumerate installed software and compare this against the authoritative software inventory. ForeScout is a platform used to scan software being used and finds software out of scope of the current inventory. Deviations from the authorized baseline will generate an alert to the System and/or Network Administrator.

10-4.7.5 Asset Inventory Integration

The software inventory must be tied to the hardware asset inventory such that all devices and the software installed on those devices can be tracked from a single location. This will allow the Postal Service to track the location of all installed software.

10-4.7.6 Authorized Application Software

The Postal Service must use authorized application technology on all assets in order to ensure that only authorized software executes and all unauthorized software is prevented from execution.

10-4.7.7 Authorized Software Library

The Postal Service authorized technology must ensure that only authorized software libraries are allowed to load into a system process. The Postal Service must use authorized software to prevent installation and execution of unauthorized software.

10-4.7.8 Authorized Software Script

The Postal Service authorized software must ensure that only authorized, digitally signed scripts are allowed to execute.

10-4.7.9 Software Segregation

The Postal Service must ensure that physically or logically segregated systems are used to isolate and run software that is required for business operations that incur higher risk for the organization.

10-4.8 Isolation of Postal Service Information

Postal Service data must not be co-mingled with non-Postal Service data.

10-4.9 Using Diagnostic Hardware and Software

Diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers) must be used only by authorized personnel for approved purposes (see 14-3, Monitoring).

10-4.10 Controlling Preventive and Regular Maintenance

Preventive and regular maintenance (and repairs) must be scheduled, documented, and controlled whether performed onsite or remotely. Information system components containing sensitive-enhanced or sensitive information must be sanitized prior to removal from a Postal Service facility. Maintenance records must be reviewed in accordance with manufacturer specifications and/or organizational requirements. Where possible automated mechanisms are employed to schedule and conduct maintenance.

Preventive and regular maintenance must be performed only by authorized personnel. When maintenance personnel do not have the needed access authorizations, organizational personnel with appropriate access authorizations must supervise maintenance personnel during the performance of maintenance activities on the information system.

Accounts used by vendors to support and maintain system components are enabled only when needed by the vendor and monitored while in use. When maintenance is complete, the security controls must be tested to ensure all security features are functioning properly.

For critical information resources, service level agreements delineate the spare parts that must be maintained onsite for the repair of key information system components and the allowable time period for repair following a failure.

10-4.11 Controlling Maintenance Tools

Information system maintenance tools must be approved, controlled, and maintained on a regular basis. Automated mechanisms are employed, where possible, to restrict use of maintenance tools to authorized personnel.

Maintenance tools brought in to Postal Service facilities must be inspected by maintenance personnel for obvious improper modifications. Media containing diagnostic and test programs must be checked for malicious code prior to use.

All maintenance equipment capable of retaining sensitive-enhanced or sensitive information must be sanitized before the equipment is removed from the Postal Service facility. If the equipment cannot be sanitized, it must remain in the Postal Service facility or be destroyed.

10-5 Configuration and Change Management

The Postal Service configuration and change management process applies to all Postal Service information resources regardless of where the information resource is hosted or managed. Security-related requirements for the following areas are presented in 8-2.4, Configuration and Change Management:

a. Configuration component inventory.
b. Standard hardened configurations.
c. Change/version control.
d. Patch management.
e. Security testing of the configuration.

10-5.1 Significant Changes

What constitutes a significant change is defined in Handbook AS-805-A, 6-2.

10-6 Protection Against Viruses and Malicious Code

All Postal Service information resources must be protected against the introduction of viruses and other types of malicious code that can jeopardize information security by contaminating, damaging, or destroying information resources. Malicious code includes harmful and other unwanted code such as viruses, worms, keystroke loggers, botnets, Trojans, trap doors, time bombs, activity trackers, remote control agents, snoopware, spyware, and adware.

10-6.1 Virus Protection Software

10-6.1.1 Installation

Information resources within the Postal Service must comply with the applicable hardening standards. Where applicable, active virus protection software must be installed, enabled, and configured to generate log files.

10-6.1.2 Scanning

To ensure Postal Service perimeter security, Information Security Services conducts scans for malicious code on the firewalls, FTP servers, mail servers, intranet servers, Internet application protocols, and other information resources such as workstations as necessary. Scans must be conducted weekly for information resources processing PCI.

10-6.1.3 Updating

Centralization of automatic updates to virus software is critical to updating information resources with the latest version of virus detection software and updated files of virus types (signature files). The managers, computing operations/infrastructures, are responsible for ensuring that virus protection software and signature files are current and distributed to Postal Service information resources. Virus protection software and signature files must be updated when received from the vendor.

10-6.2 Other Protection Measures

10-6.2.1 Protecting Shared and Retrieved Files

All personnel must run virus protection software prior to using shared or retrieved files from workstations, laptops, removable media, and other information resources.

10-6.2.2 Evaluating Dynamic Code

A code review must be conducted on sensitive-enhanced, sensitive, or critical information resources that contain dynamic code such as ASP, JavaScript, PLSQL, or CGI scripts (see 8-5.6.2, Conduct Security Code Review). In addition to the code review, information resources that contain dynamic code may be subject to an independent code review (see 8-5.6.6, Conduct Independent Security Code Review).

10-6.2.3 Protecting Applications

All application software and supporting files must be protected such that an error will be generated if there is an unauthorized attempt to modify the software. All activities involving modification of software must be logged.

10-6.2.4 Creating Backups before Installation

To assist with the post-virus restoration of normal computer activities, all computer software must be copied prior to its initial usage, and such copies must be stored in a secure location. These copies must not be used for ordinary business activities but must be reserved for recovery from computer virus infections, hard-disk crashes, and other computer problems.

10-6.2.5 Checking for Viruses Before Distribution

All software, information, or any other type of digital media must be tested to identify the presence of computer viruses and other malicious code prior to distributing to Postal Service organizations, personnel, businesses, or the public.

10-6.2.6 Intrusion Detection/Prevention

All information resources within the Postal Service must be protected against the introduction of malicious code. A layered-defense must be implemented combining network level Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Malware/URL protection, antispyware software, anti-virus software, a personal firewall, host anomaly detection/intrusion prevention software, spam and content filtering for inbound e-mail, pop-up blocker protection, and user education. Unauthorized personnel must not modify the configuration of host-based protection software.

10-6.2.7 Automated Mechanisms

Information resources must provide automated mechanisms to support the handling of information security incidents.

10-7 Operating System, Database Management System, and Application Audit Log Requirements

Operating system, database management system, and application audit logs must be sufficient in detail to facilitate reconstruction of security-related events if a compromise or malfunction is suspected or has occurred. For events where immediate attention is required, the audit utility may trigger alarms that are directed to the proper location for action.

Audit logs must be reviewed daily for potential security incidents and security breaches. The reviews may be made by automated methods. The audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified. (See 9-11, Audit Logging, for additional requirements.)

10-7.1 Operating System Audit Logs

Operating system audit logs must record security-related events. Operating systems must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of operating system integrity. Operating system software must have the capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction.

10-7.2 Database Management System Audit Logs

Database management systems must implement appropriate logging of security-related events.

10-7.3 Application Audit Logs

Sensitive-enhanced, sensitive, and critical applications that have logging capability must implement appropriate logging of security-related events.

10-7.4 PCI Audit Logs

PCI audit logs must be retained for a minimum of one year.

11 Network Security

11-1 Policy

The Postal Service network infrastructure must be protected at a level commensurate with its value to the Postal Service. Such protection must include the implementation of the physical, administrative, and technical security controls and processes that safeguard the confidentiality, availability, and integrity of the network and the data in transit in accordance with Postal Service policies and procedures. Network controls and processes are necessary to do the following:

Safeguard data traffic.

Detect and prevent unauthorized access.

Respond to computer security incidents.

Detect and correct transmission line errors.

Ensure message integrity throughout the system.

Provide network and data security.

Ensure that recovery procedures are in place and working.

Specify the appropriate auditing procedures.

The CISO enforcement policy is as follows:

a. Remediation timeline SLA.

b. Adverse action pending SLA not being met.

This policy applies to all information resources, technologies, services, and communications that are part of the Postal Service network, including the following:

a. All transmission technologies used on behalf of the Postal Service in Postal Service or non-Postal Service facilities [(e.g., local area networks (LANs); wide area networks (WANs); voice communications; videoconferencing systems; voice messaging systems; desktop video communications; satellite broadcasts; facsimile transmission; and all other transmissions over landline, wireless, or Internet-based networks].

b. All types of information and network services, data, voice, image, and multimedia communications, regardless of transmission technology.

c. Changes to mail process environment must be in accordance with Handbook AS-805 documentation. Any interaction and business conducted must be in accordance with documented processes found within Handbook AS-805G document.

The Postal Service prohibits the attachment of any non-approved network device, to include routers, switches, repeaters, wireless access-points, and

firewalls to any point of the network. Direct questions about whether a network device is approved to the NCRB via e-mail to *ncrb@usps.gov*. The Postal Service removes or disables non-approved network devices added to the network infrastructure.

11-1.1 Generic Information Security Architectural Standards Network Architecture

The Postal Service has defined generic information security architectural standards that must be adhered to when new IT products, services, or applications are purchased for use within the Postal Service IT network. There are two basic environments to be considered within the IT infrastructure:

a. Internally facing.

b. Externally facing.

11-1.1.1 Internally Facing Environment

The internally facing environment consists of hardware/software components that provide IT services to an internal only user community (e.g., Postal Service employees). In other words, the user must be on the "inside," "blue side" or ".gov" side of the Postal Service network to access the components. This environment would also permit business partner VPN and Postal Service VPN connectivity.

11-1.1.2 Externally Facing Environment

The externally facing environment consists of hardware/software components that provide IT services to an external user community. The external community is connected to the Postal Service network via a public internet connection. It is intended for Postal Service customers using Postal Service IT services such as *www.usps.com*. This community will have limited access to the "outside," "red side" or ".com" side of the Postal Service network. This environment from a network security perspective is considered hostile and extreme care must be taken to insure the Postal Service architectural standards are applied.

11-1.1.3 Enclaves, Tiers, and Zones

The basic concept of the architecture is that each environment is broken into enclaves. Enclaves are further broken down into three tiers. Specific enclaves and tier vectors can be referred to as Zones. Enclaves, tiers, and zones have degrees of separation dependent on the amount of risk each presents to the Postal Service network as a whole. The externally facing enclaves are considered high risk because they are connected directly to the internet. Enclaves with a high degree of risk use firewalls and "service separation" to provide a layered protection. Service separation, especially in the external, PCI, and sensitive-enhanced enclaves, is critical and must be understood by Postal Service application owners, hardware implementation teams, and vendors/suppliers providing services/applications to the Postal Service. Web services in the web tier must be separated from the application in the appropriate enclaves. The application must physically and logically reside on the application tier within these enclaves.

11-1.1.4 Externally Facing Websites

An HTTPS-only standard is used for all external-facing USPS web services Browsers and other HTTPS clients are configured to trust a set of certificate authorities that can issue cryptographically signed certificates on behalf of web service owners and communicate to the client that the web service host demonstrates ownership of the domain to the certificate authority at the time of certificate issuance. Internally issued certificates will not be permitted for web services whose users may not always be expected to trust the issuing federal certificate authority. These web services use a certificate issued from a publicly trusted certificate authority. The CISO is responsible for reviewing and approving, where applicable, requests for certificates from an external CA.

Externally accessible Postal Service web services must be protected through the following requirements, when available:

a. Hardening standards.

b. Application scans, code reviews, vulnerability scans, penetration testing, and vulnerability assessments.

c. Audit logs.

d. Content delivery network (CDN).

e. Web application firewall (WAF).

f. Automation/bot defense solution.

11-1.2 Network Infrastructure

The network infrastructure — facilities, equipment, services, protocols, and applications used to transmit, store, and process information — must be protected through the following requirements:

a. Physical security.

b. Network asset control.

c. Network configuration information.

d. Identification and authentication.

e. Authorization.

f. Hardening standards.

g. Secure enclaves.

h. Network isolation.

i. Vulnerability scans, penetration testing, and vulnerability assessments.

j. Firewalls.

k. Routers.

l. Demilitarized zones.

m. Network traffic monitoring.

n. Network connection.

o. Business partner and third party.

p. Remote access.

q. Network audit logs.

r. Wireless networks.

11-1.3 Wireless Network Security

Wireless technology, including wireless local area networks (WLANs), cellular technologies, radio frequency identifier (RFID) tag applications, Bluetooth technologies, and personal area networks, must be approved by the NCRB before purchase and integration.

11-2 Network Architecture

The network architecture — the appearance, functions, locations, and resources used in the network architecture — must be designed with the appropriate level of administrative and technical security controls, including the following:

a. Network addresses.

b. Network services and protocols.

c. Network perimeters.

d. Network integrity controls.

e. Time synchronization.

11-2.1 Network Addresses

All network names and addresses must be managed and approved by the central addressing authority within Telecommunications Services (TS). Internal network addresses must be protected, and access to internal network addresses is based upon a need to know and least privilege. When appropriate, TS conceals network addresses and provides translation of non-routable addresses.

11-2.2 Network Services and Protocols

All information resources must use only network services and protocols approved by the NCRB. All non-approved protocols and services must be disabled at the perimeter. Minimum requirements for extending the Postal Service intranet into the remote site are as follows:

a. Secure NCRB approval.

b. All connections to any network(s) other than the intranet must be controlled by firewalls managed by Postal Service TS or a TS designee.

c. Network changes to the agreed upon configuration must be approved by TS.

d. TS or a TS designee must have unrestricted physical access to the network.

e. All equipment connected to the network must meet current Postal Service security hardening standards.

f. Connections to the Postal Service intranet must be firewalled in a manner similar to current Postal Service secure enclave firewalling.

g. Business partner connections, including those that are an extension of the Postal Service intranet, must be Postal Service-managed via firewall or other network filtering device.

h. Passwords used to manage systems on the network must not be used to manage other systems or networks.

i. All remote site systems administrators must have a Postal Service security clearance.

11-2.3 Network Perimeters

Perimeters are clearly defined boundaries that must be established to securely control the traffic between Postal Service information resources and all other networks. All inbound or outbound network traffic must pass through appropriate access control devices, such as firewalls, before reaching Postal Service information resources. The manager, TS, must ensure perimeter monitoring and may block the Internet Protocol (IP) address of a computer performing hostile reconnaissance or attacks against Postal Service networks. Other appropriate defensive measures to protect the Postal Service information resources may be used, as approved by the manager, TS and/or the manager, CISO ISS.

Note: The Office of the Inspector General (OIG) manages, secures, monitors, scans, and supports its own network and information technology (IT) infrastructure. The OIG network connectivity to the Postal Service intranet must comply with the requirements and processes for NCRB-approved connectivity to the Postal Service intranet.

11-2.4 Network Integrity Controls

The manager, TS, establishes a system of controls to safeguard the data traffic, detect and correct transmission line errors, ensure message integrity throughout the system, and protect computers and other telecommunications endpoints. Adequate audit procedures must be employed to monitor and analyze network integrity.

11-2.5 Time Synchronization

All system (including servers) and network clocks must be synchronized to ensure all systems have the correct and consistent time

a. Based on International Atomic Time.

b. Time data is protected – access to time data is restricted and all changes to time settings are logged, monitored, and reviewed.

c. Time settings are received from an industry-accepted time source.

11-3 Protecting the Network Infrastructure

The network infrastructure consists of the facilities, equipment, services, protocols, and applications used to transmit, store, and process information. The Postal Service network infrastructure is protected through the following:

a. Ensuring physical security.
b. Maintaining network asset control.
c. Protecting network configuration information.
d. Implementing identification and authentication.
e. Implementing authorization.
f. Implementing hardening standards.
g. Determining when a secure enclave is required.
h. Establishing secure enclaves.
i. Isolating the Postal Service networks.
j. Conducting vulnerability scans, penetration testing, intrusion detection, and prevention capabilities.

11-3.1 Ensuring Physical Security

Servers and other components of the Postal Service networks must be located in areas secured to a level commensurate with the sensitivity and criticality of the information stored, processed, or transmitted. Access to network infrastructure components must be limited to authorized personnel.

11-3.2 Maintaining Network Asset Control

All infrastructure components must be inventoried at regular intervals and labeled for asset management and physical protection.

11-3.3 Protecting Network Configuration Information

Network information, including, but not limited to, configurations, addresses, subnet masks, secure enclave locations, and firewalls must be protected and treated as sensitive. Access to network configuration information must be based upon the security principles of need to know and least privilege.

11-3.4 Implementing Identification and Authentication

Personnel and information resources must be required to identify and authenticate themselves to the network before being allowed to perform any other actions on the network.

11-3.5 Implementing Authorization

Access to information resources must be granted based on the job function, appropriate clearance or background investigation, need to know, separation of duties, and least privilege.

11-3.6 Implementing Hardening Standards

Information resources supported by networking must be hardened to meet or exceed the requirements documented in Postal Service hardening standards specific to each platform. Hardening refers to the process of implementing additional software and hardware security controls. Hardening standards are based off of CIS sources, vendor recommended settings and industry best practices.

Note: The manager, CISO ISS, is responsible for the distribution of information resource hardening standards.

11-3.7 Determining When a Secure Enclave Is Required

Enclaves can be implemented to enforce separate security zones (e.g., to segregate information resources with similar issues and risks). An enclave is a virtual LAN configured to isolate a subnet/host system from other systems based on risks. All traffic in and out of the enclave is forced through a control interface.

Enclaves are required for the following information resources:

a. Information resources accessible from the Internet (i.e., externally facing information resources).

b. Information resources remotely managed by Postal Service business partners.

c. PCI information resources must be in a separate PCI compliant enclave.

d. Sensitive-enhanced information resources.

e. Sensitive and critical information resources where the risks warrant additional protection. Information resources designated as sensitive, or critical must be assessed by the manager, CISO ISS, to determine if the resource should reside in a secure enclave. A completed business impact assessment (BIA) and the architectural diagram must be submitted to the manager, CISO ISS, for review and determination of whether additional enclave protection is required.

11-3.8 Establishing Secure Enclaves

Secure enclaves are network areas where special protections and access controls, such as firewalls and routers, are utilized to secure information resources. Secure enclaves apply security rules consistently and protect multiple systems across application boundaries. Secure enclaves must be implemented as follows:

a. Place servers within the network based on the sensitivity of the data.

b. Prohibit development, SIT, and CAT servers from being on the same subnet as production servers.

c. Employ protection for the highest level of information sensitivity in that enclave.

d. Reside on network segments (subnets) separate from the remainder of Postal Service networks.

e. Use "network guardians," such as packet filtering or application proxy firewalls, to mediate and control traffic.

f. Set enclave server rules and operational characteristics that can be enforced and audited.

g. Allow only predefined, securable information traffic flows.

h. Restrict administration to a small, well-defined set of system administrators.

i. Employ intrusion detection systems and intrusion prevention systems.

j. Audit the network boundary controls through the performance of network scanning procedures on a regular basis.

k. Restrict sharing of physical devices for virtual machines among multiple enclaves.

11-3.9 Isolating Postal Service Networks

Postal Service networks must be isolated from non-Postal Service networks [e.g., business partner and vendor (supplier) networks]. Postal Service and non-Postal Service network devices must not be co-mingled. Non-publicly available Postal Service information must be isolated from non-Postal Service information (e.g., business partner and vendor information) in transit.

11-3.10 Conducting Vulnerability Scans, Intrusion Detection, Penetration Tests

Only personnel authorized by the CISO are permitted to conduct network scanning, intrusion detection, penetration testing, and vulnerability scans of Postal Service information resources. During audits and investigations, the OIG may conduct scanning, penetration testing, and vulnerability scans as deemed appropriate. The OIG has the authority to scan and conduct penetration testing and vulnerability scans on his or her own network and IT infrastructure. Reports resulting from these vulnerability actions are sent to the program managers with a copy to the Corporate Information Security Office/ISSO for each system. The ISSOs will include these vulnerabilities into Risk Mitigation Plans for each system or Risk Register.

11-3.10.1 Vulnerability Scans

Vulnerability scans are required to systematically examine an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Requests for vulnerability scans must be directed to the manager, CISO ISS, for approval. Vulnerability scans are conducted on Postal Service information resources by CISO ISS or their designee.

11-3.10.2 Intrusion Detection and Protection

Intrusion detection is required to monitor network and/or system activities for malicious activity. The main functions of intrusion detection/prevention are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. All policy configurations will be managed by CISO ISS.

Requests for intrusion detection must be directed to the manager, CISO ISS, for approval. Intrusion detection is conducted for Postal Service networks by CISO ISS or their designee. The OIG conducts intrusion detection at its discretion.

The intrusion detection process consists of the following:

a. Monitor the network for suspicious traffic.

b. Examine network traffic to identify threats.

c. Utilize one of three detection methods:

(1) Signature-based detection.

(2) Statistical anomaly-based detection.

(3) Stateful protocol analysis detection.

(4) Dynamic analysis.

d. Take appropriate actions to mitigate the detected threats. This includes, but is not limited to, the following:

(1) Produce alert.

(2) Reset current session with/without alerts.

(3) Drop current session with/without alerts.

11-4 Internet Technologies

The Postal Service uses Internet technologies in the following environments:

a. Internet.

b. Intranet.

c. Extranet.

11-4.1 Internet

Access to the Internet from Postal Service information resources must be routed through Postal Service-approved access control technology (e.g., firewalls, proxies and IPS).

11-4.2 Intranet

An intranet is a network based on Internet technologies located within an organization's network perimeter. The Postal Service operates and maintains an intranet for the conduct of Postal Service business. Access control technology, such as firewalls and filtering routers, IDS, and IPS, must be used to protect the Postal Service intranet at the network perimeter to provide access control and support for auditing and logging.

11-4.3 Extranet

An extranet is a network based on Internet technologies that allows an organization to conduct business and share information among business partners, vendors (supplier), and customers. Business partners must comply with the requirements and process of the NCRB contained in the Handbook AS-805-D, *Information Security Network Connectivity Process*. Business partners must be limited in their access to the specific information resources identified in the network connectivity request that is approved by the NCRB.

11-5 Protecting the Network/Internet Perimeter

The perimeter between the Postal Service network and the Internet environments must be protected through the following:

a. Implementing Internet security requirements.

b. Implementing firewalls.

c. Implementing routers.

d. Establishing demilitarized zones (DMZs).

e. Implementing IDS/IPS services.

f. Monitoring network layer traffic.

g. Monitoring and inspecting application layer traffic.

11-5.1 Implementing Internet Security Requirements

Internet-accessible information resources, such as those residing on DMZs, must implement security requirements that include, but are not limited to, the following:

a. Securely partitioning each Internet-accessible environment (e.g., the intranet and extranet) from each other.

b. Using firewalls or filtering devices to screen and monitor incoming and outgoing traffic.

c. Supporting encryption to protect the storage and transmission of sensitive-enhanced and sensitive information.

d. Performing continual evaluation, testing, monitoring, and maintenance of the firewalls.

e. Applying real-time monitoring, auditing, and alerting to detect intrusion, fraud, abuse, or misuse.

Access control technology, such as firewalls and filtering routers, must be used to protect the Postal Service intranet at the network perimeter to provide access control and support for auditing and logging.

11-5.2 Implementing Firewalls

A firewall is a safeguard or type of gateway that is used to control access to information resources. A firewall can control access between separate networks, between network segments, or between a single computer and a network. A current-generation firewall is generally not a single component but a strategy composed of both hardware and software for protecting an organization's resources.

Direct public access between the Internet and the Postal Service intranet must be controlled by a firewall. A firewall must be installed at each Internet connection and between any DMZ (and all PCI enclaves) and the Postal Service intranet.

Secure NCRB approval in advance of establishing network connectivity to an information resource involving firewall changes.

Firewalls must implement Postal Service hardening standards. These hardening standards must be updated as new vulnerabilities are uncovered

and updates are available. Firewall hardening standards must be reviewed and updated at least annually.

A firewall must also be installed at each connection between the Postal Service intranet and mail processing equipment and mail processing infrastructure (MPE/MPI) devices. MPE/MPI firewall rule changes do not require NCRB approval.

11-5.2.1 Firewall Configurations

Postal Service firewalls must be configured to do the following:

a. Deny all services not expressly permitted (i.e., deny all inbound and outbound traffic not specifically allowed).

b. Restrict inbound Internet traffic to Internet Protocol (IP) address with the DMZ (ingress filters).

c. Prevent internal addresses from the Internet into the DMZ. Use anti-spoofing commands and techniques to prevent internal addresses from being spoofed and passed from the Internet to the DMZ.

d. Implement dynamic packet filtering (i.e., only allow "established" connections into the network).

e. Secure and synchronize router configuration files (i.e., running configuration files and start-up configuration files used to reboot machines must have the same secure configuration).

f. Audit and monitor all services to detect intrusions or misuse.

g. Notify the firewall administrator and system administrator in near real time of any item that may need immediate attention.

h. Run on a dedicated computer.

i. Stop passing packets if the logging function becomes disabled.

j. Disable or delete all nonessential firewall-related software, such as compilers, editors, and communications software.

11-5.2.2 Firewall Administrators

Each firewall or logical group of firewalls must have adequate resources assigned for firewall administration. Firewall administrators are responsible for ensuring compliance with standards for configuration and approved services and protocols.

11-5.2.3 Firewall Administration

All Postal Service firewalls must be located in a controlled environment. Firewall configuration standards must include a description of roles and responsibilities for management of all components.

Firewall administration must be performed from the local console or via remote access if approved by the manager, CISO ISS, and appropriately secured through strong authentication and encryption. Firewall configurations must be protected and treated as sensitive. Access to firewall configuration information must be based upon the security principles of need to know and least privilege.

11-5.2.4 Firewall System Integrity

Firewall rule sets must be reviewed every 6 months. Firewall system configuration and integrity must be validated and tested monthly by the firewall administrator.

11-5.2.5 Firewall Backup

The firewall (e.g., system software, configuration data, and database files) must be backed up as determined in the appropriate business continuity plan.

11-5.3 Implementing Routers

A router is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. Routers connect two or more logical subnets, allowing interconnectivity with hosts on intranets and extranets.

11-5.3.1 Router Configurations

Postal Service routers must be configured to do the following:

a. Implement Postal Service network security controls.

b. Suppress router advertisements.

c. Disable the finger service on all routers.

d. Disable File Transfer Protocol [FTP] server on all routers.

e. Disable Hypertext Transfer Protocol [HTTP] server on all routers.

f. Disable the boot-up service on all routers.

g. Disable configuration auto-loading on all routers.

h. Disable Internet Protocol [IP] source routing on all routers.

i. Disable IP directed broadcasts when not required.

j. Disable service Packet Assembler Disassembler [PAD] on all routers.

k. Disable proxy Address Resolution Protocol [ARP] when not required.

l. Disable gratuitous ARP on all routers.

m. Disable Simple Network Management Protocol [SNMP] write access to the router.

n. Disable Transmission Control Protocol [TCP] and User Datagram Protocol [UDP] small server services.

o. Disable Berkley Software Distribution [BSD] commands on remote systems.

p. Enable TCP keep-alive messages.

q. Enable Cisco Express Forwarding (CEF) on all Cisco routers.

r. Filter Internet Control Message Protocol [ICMP] on external interface.

s. Configure Data Name System [DNS] servers as a client resolver.

t. Configure virtual private network [VPN] as a tunnel type VPN.

u. Log severity levels 0 through 6.

v. Block IPv6 routing header.

w. Block IPv6 Undetermined Transport.

x. Block inbound traceroute responses.

y. Block RFC1918 addresses.

z. Set routers to intercept TCP SYN attacks.

aa. Limit TCP connection request wait times.

ab. Restrict access to stored configuration files.

ac. Restrict IPSec traffic.

ad. Require a log or syslog statement that follows every deny, discard, or reject statement.

ae. Require all network infrastructure component resources have latest operating system release level.

af. Require SNMP version 3 or higher be installed.

ag. Restrict SNMP access by IP address.

ah. Block SNMP at all external interfaces.

ai. Classify and mark management traffic to ensure it receives preferred treatment at each forwarding device along the path.

aj. Restrict messages to the Syslog Server.

ak. Synchronize Run and Startup configurations.

al. Configure Console Port to time out in 15 minutes or less.

am. Encrypt In-band traffic.

an. Log In-band management access attempts.

ao. Configure SSH timeout to 60 seconds or less.

ap. Implement SSH Version 2.

11-5.3.2 Router Administration

Router rule sets must be reviewed at least every six months.

11-5.4 Establishing Demilitarized Zones

DMZs are network segments between intranets, extranets, and the Internet that provide increased security for data transfer between information resources, vendors (supplier), and the public. DMZ requirements include the following:

a. Web servers and electronic commerce systems accessible to the public must reside within a DMZ with approved access control implemented via a firewall or gateway.

b. Sensitive-enhanced, sensitive, and critical information must not reside within the DMZ. Sensitive-enhanced, sensitive, and critical information must be installed on an internal network zone (i.e., enclave segregated from the DMZ).

c. All inbound traffic to the intranet from the DMZ must be passed through a proxy-capable device.

d. Virtualization is not allowed in the DMZ.

11-5.5 Monitoring Network Traffic

The Postal Service network perimeter must be monitored for network connectivity, services, and traffic. Monitoring must be conducted on both active and inactive connections.

Firewalls and IDS/IPS should be part of the path requirements as part of Compliance and Monitoring requirements as follows:

a. 11-7, BP connectivity requirements.
b. 11-8, Third-Party network connectivity.
c. 11-9, Remote access requirements.
d. 11-11, Wireless Network requirements.

11-6 Network Connections

11-6.1 Establishing Network Connections

The NCRB must approve all system network access before connectivity is established to the USPS network. Systems with high or moderate impact values with respective confidentiality, integrity, or availability security objectives have unique identity and authenticate network devices before establishing a connection to the USPS network. All connectivity to the USPS network must be monitored and audited in advance of the establishment of network connectivity. Any connectivity to the Postal Service network must allow monitoring.

11-6.2 Requesting Connections

The NCRB provides the mechanism for requesting, reviewing, evaluating, and approving connectivity between non-Postal Service individuals and organizations wishing to establish connectivity to the Postal Service intranet.

11-6.3 Approving Connections

Requests for connectivity to the Postal Service intranet must be reviewed, evaluated, and approved by the NCRB. All requests for connectivity must follow and comply with the requirements identified in the NCRB request process described in Handbook AS-805-D.

11-6.4 Physical Protection of Network Connections

Physical access to publicly available network jacks must be restricted to authorized personnel and enabled only when needed. Disable unused network connections in areas such as conference rooms where visitors and unauthorized network users are not escorted.

11-7 Business Partner Connectivity Requirements

Business partner/contractor/supplier (business partner) connectivity must be requested and funded by a Postal Service sponsor.

Connections using either existing BP ISP connectivity or frame relay service directly connected to the Postal Enterprise are protected by firewalls and security processes that restrict business partners to the IP address or addresses, server or servers, and ports or protocols they are explicitly authorized to access.

Business partners must be limited in their access to the specific information resources identified in the network connectivity request that is approved by the NCRB. No business partner is ever granted "open access" to Postal Service computing resources. These connections must be based on least privilege for both source and destination address. The use of blanket rules, such as wildcard masks and subnets larger than /24, will not be permitted without additional approval.

To protect the integrity of the Postal computing environment, business partners must have written information security policies describing how they will protect their proposed connection to the Postal Service and must include a copy of these security policies with their NCRB request.

Business partners must comply with the requirements and process of the NCRB contained in the Network Connectivity Process including, but not limited to, the following:

a. Initiating requests with the executive sponsor for access to the Postal Service intranet.

b. Complying with all Postal Service information security policies.

c. Allowing site reviews by the Inspection Service or CISO.

d. Allowing audits by the OIG.

e. Reporting any security incident immediately to CyberSafe and executive sponsor.

f. Notifying the executive sponsor when connectivity is no longer required.

g. The executive sponsor will notify CISO/NCRB and open a request to remove access within 7 days of connectivity no longer being required (SLA).

11-8 Limiting Third-Party Network Services

Network services approved for third-party connectivity must be governed by the principle of least privilege and limited to those services and devices needed to perform the business function requested. The default must be to deny all access except those services specifically approved by the NCRB. The default must be to deny all access except those services specifically approved by the NCRB. The principle of least privilege applies to both source and destination addresses. The use of blanket rules such as wildcard masks and subnets larger than /24 will not be permitted without additional levels of approval.

When establishing third-party connections, access controls and administrative procedures must be implemented to protect the confidentiality of Postal Service information resources. The third party must be responsible for

protecting its private network infrastructure and information and must not rely on the Postal Service to perform this function. Part of securing the connection should include the Postal Service ability to monitor and inspect traffic.

11-9 Remote Access Requirements

Remote access privileges are restricted to authorized personnel and must be approved by appropriate management through eAccess/ARIS before being granted. Remote workstations and laptops must be physically secured to prevent unauthorized access to the device and the Postal Service intranet. The use of personal information resources to remotely connect to the Postal Service intranet must be approved and connectivity must be managed through an approved virtual private network (VPN) solution.

An automatic session disconnect must be implemented for remote access technology after the standard time-out requirement. (See 9-6.10.3, Time-Out Requirements (Re-authentication) for the standard.)

11-9.1 Authentication

Information resources should be capable of strong authentication on application or network connections requiring remote access. Remote access requires users or devices to authenticate at the perimeter or connect through a firewall. Remote user communications must occur through encrypted VPN channels. Where possible, the authentication should use eAccess/ARIS. Remote PCI-related access must implement two-factor authentication.

11-9.2 Virtual Private Network

A VPN provides end users with a way to securely access information on the Postal Service intranet over an untrusted network infrastructure or an untrusted public network such as the Internet. Postal Service VPN requirements include, but are not limited to, the following:

a. Any Postal Service VPN solution must provide end-to-end encryption and strong authentication capability.

b. Employees must submit an electronic request for computer access, or its equivalent, to obtain access to Postal Service information resources through a VPN.

c. Business partners requiring access to Postal Service information resources through a VPN must submit a formal request to the NCRB in accordance with Handbook AS-805-D, *Information Security Network Change Process.*

d. Any VPN solution used for business partner connectivity must be capable of filtering access to specific information resources, and the connection must allow monitoring.

e. Any computing device connecting to the Postal Service intranet through a VPN must implement an approved personal firewall configured to Postal Service standards, as defined by CISO.

f. The end user must use a Postal-approved device or remote connection method and has the responsibility to gain access and fund the Internet Service Provider (ISP) service when accessing Postal Service resources. The Postal Service does not provide recommendations for any local ISP access. Once a communication path to the Internet through the ISP has been established, the VPN session is initialized through the Internet to the Postal Service network.

g. Upon management approval, contractors with unique Active Directory (AD) credentials and two-factor authentication may use a shared ACE computer where work requirements do not support the assignment of an individual ACE computer.

11-9.3 Modem Access

Modem access for all information resources to and from Postal Service networks must be approved in writing in advance by the manager, CISO ISS, and must implement the information resource protection measures described below.

Note: Additional modem approval by the manager, CISO ISS, is not required for approved remote access services (e.g., VPN or point-to-point protocol (PPP).

Any workstation on the Postal Service intranet with approved modem access must:

a. Implement an approved personal firewall configured to Postal Service standards as defined by CISO ISS.

b. Disconnect from the Postal Service intranet prior to establishing alternate or additional connections to any network such as the Internet.

c. Initiate protection measures to ensure that the system has been cleaned of any malicious code prior to being permitted to connect to the Postal Service infrastructure.

d. Deactivate modem immediately after use.

11-9.4 Dial-in Access

All dial-in access to and from Postal Service networks must be approved in advance by the responsible Postal Service manager and implemented by the manager, TS. All approved dial-in access must be established through Postal Service centralized dial-in services.

11-9.5 Telecommuting

Personnel working at alternative work sites must only use Postal Service approved computer hardware, software, and virus protection software when working on Postal Service business, when sharing files with the Postal Service, or when communicating through phone lines or the Internet with the Postal Service. Any approved personal hardware must have the latest security patches installed, Postal Service-approved virus software installed with the latest pattern recognition file, and, if connecting via the Internet, a Postal Service-approved personal firewall must be implemented.

11-9.6 Remote Management and Maintenance

To protect the integrity of the Postal computing environment, use of remote administration and maintenance software and associated security controls must be approved by the manager, CISO ISS, in cooperation with the requesting organization.

Remote management and maintenance must be controlled and activity logs maintained. The remote access links, frequency of access, and associated controls must be documented in the security plan for the information resource. Two-factor authentication must be implemented and all communications must be encrypted. Vendor maintenance accounts must be enabled only when needed. When remote management and maintenance is completed, the remote access connection must be disconnected and disconnection verified.

Organizations performing remote access must implement the same general level of security as the system being accessed. Instances of remote management and maintenance must be audited on a regular basis.

11-10 Network Audit Log Requirements

Networks including firewalls and controlled interfaces must have an audit capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction. Network audit logs must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of network integrity. Network audit logs must be sufficient in detail to facilitate reconstruction of security-related events if a compromise or malfunction is suspected or has occurred. For events where immediate attention is required, the audit utility must trigger alarms that are directed to the proper location for action.

Network audit logs must be reviewed daily for potential security incidents and security breaches. The reviews may be made by automated methods. Audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified. (See 9-11, Audit Logging, for additional requirements.)

11-11 Wireless Networking Requirements

Wireless devices and the supporting network infrastructure are subject to the following wireless security requirements and standards: a. Wireless baseline requirements.

b. Wireless solutions.

c. Standard wireless solution.

d. Process for requesting nonstandard wireless solutions.

e. Bluetooth and personal area network applications.

f. Wireless LAN device management.

g. Compliance and monitoring requirements.

h. Firewalls and IDS/IPS.

Note: This policy does not cover wireless devices (e.g., cellular phones, pagers, and radio systems) unless they transmit data (see MI AS-8602003-2, Data Stewardship: Data Sharing Roles and Responsibilities).

11-11.1 Wireless Baseline Requirements

The following baseline requirements are key to ensuring basic functionality, maximum bandwidth, and appropriate network security:

a. Wireless applications must be capable of "mutual" device and user authentication (i.e., the device, the user, and the network must recognize each to be who they say they are).

b. There must be a secure link between a device and an access point (AP).

c. In addition to approval by the EAC, all wireless technology must be approved by the Spectrum Management Office before any implementation activities are initiated.

d. The installation of access points, wireless cards, or any wireless technology must be approved in advance by the manager, Telecommunication Services, and the NCRB because of the risks such installations can introduce to the Postal Service intranet, networks, and all connected information resources.

e. Telecommunications Services is authorized to deploy the standard wireless solution without additional approvals.

f. Wireless and wired networks must be developed and maintained separately and distinctly. A firewall is required between the wired and wireless network segments if Postal Service certificates are not used to Connecting APs or using wireless technology without proper prior approval introduces an unacceptable risk to the Postal Service intranet and other assets. Non-approved wireless technology must be removed from the Postal Service computing environment.

11-11.2 Wireless Solutions

Wireless technologies enable one or more devices to communicate without physical connections — without requiring network or peripheral cabling. Wireless technologies use the radio frequency spectrum to transmit data and such technologies present security-related challenges. Wireless solutions are grouped as follows:

a. Standard wireless solution.

b. Nonstandard wireless solution.

Devices that meet the current WLAN standard solution do not require a firewall between wireless devices and wired networks. All other devices require a firewall between wireless devices and wired networks.

11-11.3 Standard Wireless Solution

11-11.3.1 General Requirements

This standard technology solution is predicated on the implementation of the following general requirements:

a. Assurance that the device is authorized to access the Postal Service network domains.

b. Assurance that it is a Postal Service-managed device using approved virus protection, security patches, and personal firewalls.

c. Authentication of the user through Active Directory (AD) credentials.

d. Mutual authentication of device/client and remote authentication dial-in user service (RADIUS) server through Postal Service internal Certification Authority (CA) machine certificates.

11-11.3.2 Architecture Requirements

Wireless solutions must be compliant with the Mobile Computing Enterprise Architecture. The complete Architecture document can be found in the following documents folder: *http://it.blueshare.usps.gov/sites/itmc/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitmc%2FShared%20Documents%2FMobile%20Architecture%20and%20Strategy%20Documents*

Technical requirements for standard wireless architecture solutions are:

a. The standard architecture for WLAN authentication/encryption must be a Postal Service device capable of using:

(1) A Postal Service internal CA machine certificate authenticating to AD.

(2) Temporal key integrity protocol (TKIP) encryption.

(3) Wi-Fi Protected Access 2 (WPA2) or higher based on best practices for key management.

(4) Application and network device owners using PKI-based encryption on any wireless device implement and maintain a key management plan as identified within this policy document and approved by CISO.

b. Users must authenticate to AD and be authorized for wireless access.

c. Users and devices must be registered members of AD.

d. Users must be able to authenticate using AD credentials.

e. Devices such as workstations must be able to mutually authenticate to a RADIUS server using Postal Service Internal CA certificates.

f. The technology solution must use an approved supplicant client and the device must be a Postal Service device.

g. Clients must be able to download, store, and use a Postal Service internal CA machine certificate.

h. Protocols (e.g., PEAP) capable of supporting Postal Service machine certificates must be used.

i. Workstation/wireless card clients must be registered for central device management.

j. Drivers and cards must be compatible with Postal Service standards and certified by TS for use within the Postal Service network.

k. Service set identifier (SSID) standardization must be implemented to support mobility.

l. Firewall segmentation must be implemented at the demarcation of wireless networks to mitigate the risk of attack through compromised wireless networks.

11-11.3.3 How to Request Standard Wireless Services

Standard wireless connectivity is requested as follows:

a. Wireless infrastructure must be requested through TS.

b. Wireless infrastructure must be deployed, documented, and managed by TS.

c. Wireless cards/client devices must be purchased via Postal Service processes and contracts. The acquisition of mobile computing devices must be approved through IT Mobile Computing.

d. User wireless services must be requested via eAccess/ARIS at *https://eaccess.usps.gov*

11-11.4 Process for Requesting Nonstandard Wireless Solutions

The following process must be followed for business solutions including the use of wireless technology that do not meet the standards previously defined:

a. Obtain NCRB approval to proceed. Before pursuing a nonstandard wireless technology solution, approval to proceed from the NCRB must be obtained. The NCRB requires a business case for the alternate solution. The NCRB dictates the non-negotiable standards that the alternate solution must be compliant with.

b. Develop an architecture design. Develop an engineering architectural design in conjunction with TS. TS should validate compliance and functionality of the design to ensure that it will not adversely affect the current Postal Service solutions. TS will submit the solution design to IT Mobile Computing for review to ensure compatibility with the overall managed mobile computing technical architecture and strategy.

c. Obtain NCRB approval of the architectural design.

(1) Obtain approval of the application, the engineering architecture, and all wireless devices from the NCRB.

(a) For implementations involving MPE/MHE, contact the responsible design engineering organization that will send an e-mail to *NCRB@email.usps.gov* or submit a request through the NCRB Web site. The design engineering organization may also present the MPE/MHE project to the NCRB.

(b) For other implementations, contact the Business Relationship Management portfolio manager who will send an e-mail to *NCRB@email.usps.gov* or submit a request through the NCRB Web page on the IT Web. The Business Relationship Management portfolio manager will also act as a presenter to the NCRB on the requestor's behalf.

(2) At a minimum, the NCRB will evaluate against the following criteria prior to approval for implementation of wireless technology:

(a) Proper naming with regards to SSID.

(b) SSID broadcast turned off.

(c) Encryption of data between a device and an access point, or an ancillary downstream device. The majority of wireless APs have some inherent encryption capabilities.

(d) Trust between wireless devices. When setting up APs, there should be appropriate authentication — particularly a mutual authentication mechanism between a wireless device and an access point (802.1x) and user-based authentication when applicable (i.e., two-factor).

(e) Appropriate logging/intrusion detection on the wireless segment, either on the access point or related device.

(f) The requirement for whether a firewall is needed between the wireless AP and WAN.

(g) Centralized, secure administration using unique user name and passwords that are compliant with Postal Service policy. Ideally, all wireless user accounts should be located in a common repository.

(h) Firewall and virus protection implementation on devices.

(i) Request through eAccessARIS if Postal Service Internal CA machine certificates are required.

(j) Devices are remotely manageable by TS.

d. Obtain a wireless site survey. A wireless site survey must be performed to obtain maximum benefit of the wireless devices and to maintain appropriate security. TS arranges for the site survey via the Postal Service intranet contract. Normal turn-around time is 62 days; expedited is 30 days. The survey results will place the APs, offer channel sections, and specify other physical and programming parameters.

e. Acquire, program, and install device. After NCRB approval and review of the site survey report, the wireless infrastructure devices may be purchased by the customer through TS, who will then configure the devices. When the devices are programmed, they are sent to the site ready to be installed by the Postal Service intranet vendor.

11-11.5 Bluetooth and Personal Area Network Applications

Postal Service initiatives using Bluetooth and personal area networks require approval from the NCRB prior to deployment.

All implementations of Bluetooth and personal area networks must meet the requirements for a nonstandard wireless solution and the following requirements:

a. Radio frequency range must be managed, using only the minimum signal required, to perform the task and checked semiannually for confinement.

b. Device pair bonding (mutual authentication) must be used. Ensure the Bluetooth bonding environment is secure from eavesdroppers. If the authenticator (e.g., PIN, password, and shared secret) meets Postal Service aging and storage requirements, the standard password criteria apply (see 9-6.1, Passwords), otherwise the authenticator must be complex and a minimum of 16 characters.

c. The link between devices must be encrypted during the authentication exchange process and also when sensitive-enhanced or sensitive information is transmitted. Use security mode 3.

d. Bluetooth or personal area networks configuration files must be checked semiannually to ensure the security policy is enabled on devices where the files are accessible by end users.

e. Personal use of Bluetooth on Postal Service premises must be approved by the user's vice president or his or her designee because of the potential for interference to Postal Service systems such as Surface Visibility and Yard Management.

11-11.6 Wireless LAN Device Management

TS or its designee remotely manage all devices that connect to the network using 802.11x technology, that incorporate TACACS, and have RADIUS authentication. Periodic software updates and product enhancements are downloaded to APs as required to improve performance and enhance security. Access point management also includes constant operating assessments of the device. Any malfunctions or loss of effectiveness generate an alert for resolution.

11-11.7 Purchasing Requirements

Purchasing requests for wireless hardware, software, and services must address the requirements stated in items a through s below in order to comply with the Postal Service wireless security policy. For any particular wireless application, all of the requirements may not apply. The security requirements should be included in purchasing specifications procurement documents to adequately protect the wireless application and reduce the residual risk to an acceptable level.

Procurements must be compatible with the Mobile Computing Enterprise Architecture. An extract of the Best Practices and Standards can be found in the following documents folder: *http://it.blueshare.usps.gov/sites/itmc/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitmc%2FShared%20Documents%2*

FMobile%20Architecture%20and%20Strategy%20Documents

Wireless devices should be capable of supporting the following requirements:

a. For devices intended for stationary deployment (e.g., in vehicles or on loading docks), capable of being solidly secured (e.g., to the vehicle or building). This requirement also applies to add-on modules.

b. Capable of requiring a "power-on" password prior to the device operating. This password is in addition to the specific user authentication password.

c. Capable of ensuring device authentication and strong (at least two-factor) user authentication. The wireless device must have the capability to be configured to query a secondary device for access when the primary server is offline.

d. Be Wi-Fi protected access (WPA) certified. Has built-in security features, including data link-level encryption, 802.1x-compliant authentication model, and regular rotation of encryption keys.

e. Contain secure authorization software/firmware.

f. Where extensible authentication protocol (EAP) is used, capable of proper password management (e.g., aging and complexity criteria). The wireless device must have the capability to support password changes in a pre-established timeframe.

g. Capable of ensuring that users can be securely authenticated when operating locally or remotely. The device automatically senses when it is operating in a connected manner and uses the proper authentication.

h. Capable of implementing mutual authentication between the device and an access point.

i. Capable of being Active Directory-compliant for authentication purposes. Exceptions must be documented.

j. Capable of logging events.

k. Capable of meeting the Postal Service minimum encryption standard.

l. Capable of providing a secure channel for access point administration.

m. Capable of supporting end-to-end cryptographic protection for transmitting sensitive-enhanced and sensitive information where the traffic traverses network segments other than the wireless segment.

n. Capable of dynamic encryption key rotation. The wireless device must have the capability to support rotation of encryption keys in a pre-established timeframe.

o. Capable of supporting a timeout mechanism that automatically prompts the user for a password after a period of inactivity. The period of inactivity must be configurable via the device set-up procedure and ignore the keep-alive process (pings or loop socket-to-socket packets) for automated programs.

p. Capable of deactivating all communication ports and network associations during periods of inactivity.

q. Capable of implementing a personal firewall on wireless clients.

r. Capable of supporting static IP addresses and dynamic host configuration protocol (DHCP) on remote wireless equipment.

s. Capable of shielding authentication credentials against interception through short interval "authentication tunnels" (i.e., TLS standard).

Technical support for the integration of the wireless devices into the Postal Service infrastructure with other technological initiatives must be scoped, planned, and available in a timely and accurate manner (e.g., remote access for MPI, structured wiring switches, and SEF access).

11-11.8 Deployment Requirements

It is imperative to carefully plan the deployment of wireless technology. It is much more difficult to address security once deployment and implementation have occurred; therefore, security should be considered from the initial planning stage through deployment and operation.

Fulfilling the requirements stated in this section will ensure compliance with the Postal Service wireless security policy. For any particular wireless application, all of the requirements may not apply. The information systems security officer (ISSO) must work with the executive sponsor to select the security requirements that must be implemented to adequately protect that application and reduce the residual risk to an acceptable level.

11-11.8.1 Administrative Security Requirements

Wireless infrastructure administrative security controls and management practices are crucial to operating and maintaining a secure wireless network. Wireless administrative security requirements are:

a. Do not install access points, wireless cards, or wireless devices to gain access to the Postal Service intranet without prior written approval from the NCRB.

b. Submit a detailed Security Plan to the NCRB along with the request for wireless connectivity.

c. Implement configuration/change control to ensure that equipment (e.g., access points) has the latest software release that includes security feature enhancements and patches for discovered vulnerabilities.

d. Review security-related mailing lists for the latest security vulnerabilities and alerts and respond accordingly.

e. Test software patches and upgrades.

f. Install security patches in a timely manner (within 30 days for information resources supporting PCI applications).

g. Use approved standardized configurations that reflect the information security policy and hardening standards to ensure consistency of operation.

h. Change system defaults that come with the wireless access points, including SSID, password, read/write community strings, and IP addresses set by the manufacturer.

i. Implement firewalls between access points and the wired network.

j. Conduct scans continuously to identify unauthorized access points and other devices that can disrupt the wireless network or compromise the security of the Postal Service intranet. For the PCI cardholder environment, the scans must be conducted quarterly.

k. Disable wireless devices not included in the authorized wireless inventory.

l. Conduct information security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies (including the fact that robust cryptography is essential to protect the "radio" channel, and that theft of equipment is a concern).

m. Ensure that users know where to report lost or stolen wireless devices.

n. Perform a risk assessment to understand the value of the assets that need protection and document the residual risk following the application of all security countermeasures in the wireless deployment.

o. Centralize wireless security administration and actively monitor user connections.

p. Turn off communication ports and network associations during periods of inactivity when possible.

q. Perform perimeter surveys to review and adjust radio transmit power settings to prevent spillover (i.e., the leakage of Postal Service wireless radio signals beyond the perimeter of Postal Service property).

r. Use non-intelligible SSID identifiers, cryptographic keys, and administrative passwords.

s. Access point information fields must not be populated with Postal Service-identifiable information.

t. Bridging must always be disabled on access points and on remote wireless equipment that also has wired connectivity.

u. Disable SSID broadcasts on all wireless equipment.

v. Minimize broadcasts from access points or broadcasts on a segment (e.g., access point connected to a wired hub), and limit access point associations.

w. Ensure no microwave ovens or cordless phones are within sufficient range to create interference on WLANs.

x. Install antivirus software and malicious and unauthorized content inspection monitors on portable wireless devices.

y. Ensure access control lists clearly identify application rights (authentication) for all wireless users.

z. Avoid placing sensitive-enhanced or sensitive information on a handheld device. Store sensitive-enhanced or sensitive information encrypted and delete it from the handheld device when no longer needed.

aa. Synchronize mobile wireless devices with the corresponding workstations regularly.

ab. Do not use Postal Service-owned equipment on home wireless networks without a personal firewall and virus protection.

11-11.8.2 Physical Security Requirements

Physical security controls should be implemented to mitigate some of the risks such as theft of equipment and insertion of rogue access points, including wireless network monitoring devices. Physical security controls (e.g., barriers, access control systems, and guards) are the first line of defense. Wireless physical security requirements are as follows:

a. Deploy physical access controls (e.g., photo ID, card badge readers) to the building and other secure areas to protect against tampering and theft.

b. Solidly fix devices not under continuous user control (e.g., left in vehicles or on loading docks) to the vehicle or building through the use of physical locks and cables to minimize the risk of loss or theft.

c. Stow handheld devices in locked rooms and cabinets especially when left unattended for long periods (e.g., overnight).

d. Secure add-on modules to minimize the risk of loss or theft, since they sometimes are as much of a target as the primary handheld device.

e. Ensure access points are physically secure from tampering.

f. Locate authentication servers in protected areas behind access points.

g. Where sensitive-enhanced or sensitive information is transmitted, ensure external boundary protection (e.g., a fence or locked doors) is in place around the perimeter of the building or buildings.

11-11.8.3 Technical Security Requirements

Technical security controls should be implemented to mitigate risks such as eavesdropping, traffic analysis, masquerading, replay, message modification, and denial of service. Wireless technical security requirements are as follows:

a. Implement a "power-on" password based on Postal Service standards for each mobile wireless handheld device.

b. Implement appropriate password management (e.g., aging) for all handheld devices.

c. Implement mutual authentication between a wireless device and an access point.

d. Implement authentication for users whether operating locally or remotely (i.e., authenticate to the device or to the network).

e. Provide only specific services (e.g., HTTP, HTTPS, and SMTP).

f. Control access between the WLAN and wired LAN with a firewall.

g. Implement timeout mechanisms that automatically prompt the user for a password after a period of device inactivity.

h. Implement nonrepudiation access check for financial transactions.

i. Use the wireless access point for access only.

j. Configure the wireless access point properly.

k. Set wireless access points at 1, 6, and 11 so they do not compete and interfere with each other. If a nonstandard channel is used, it will indicate a possible "man-in-the-middle" attack.

l. Routinely test the inherent security features (e.g., authentication and encryption) that exist in wireless algorithms to protect sensitive-enhanced and sensitive information.

m. Encrypt data between a device and an access point, or ancillary downstream device utilizing Postal Service minimum encryption standards.

n. Use a VPN to secure communication between WLAN and LAN resources.

o. Implement mandatory access control (MAC) address filtering.

p. Use a HTTP/SHTTP proxy to access the Internet.

q. Turn off ad hoc networking and ensure your wireless network interface card (NIC) remains in "infrastructure only" mode.

r. Use temporal key integrity protocol (TKIP) to provide data encryption including a pre-packet key mixing function, a message integrity check (MIC), an extended initialization vector with sequencing rules, and a rekeying mechanism.

s. Implement 802.1x and EAP to provide a framework for strong user authentication.

t. Employ Postal Service standard end-to-end cryptographic protection to transmit sensitive-enhanced and sensitive information over other network segments, including wired segments or the Internet.

u. Even when approved cryptography is used, employ additional countermeasures (e.g., strategically locating access points, firewall filtering, blocking, and installation of antivirus software) as required.

v. Employ automated key rotation.

w. Install personal firewall software on all mobile networked wireless devices.

x. Implement appropriate logging and intrusion detection where any wireless equipment is used.

11-11.8.4 Maintenance Security Requirements

Maintaining a secure wireless network and associated devices requires significant effort, resources, and vigilance. Wireless maintenance security requirements are as follows:

a. Maintain a full topology of the wireless network.

b. Label and keep inventories of the fielded wireless and handheld devices including MAC addresses and serial numbers.

c. Create frequent backups of data on mobile wireless equipment.

d. Perform quarterly security testing and vulnerability assessments of the wireless network.

e. Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.

f. Apply patches and security enhancements in a timely manner (within 30 days for information resources supporting PCI applications).

g. Vigilantly monitor wireless technology for new threats and vulnerabilities.

h. Install the latest antivirus software on mobile wireless equipment.

i. Implement a secure channel for access point administration.

j. Configure alerts to data volume, packet collisions, and retries.

k. Conduct site surveys and adjust radio transmit power settings to avoid transmissions beyond Postal Service-owned property.

l. When disposing of handheld devices that will no longer be used, sanitize memory to prevent the disclosure of sensitive-enhanced or sensitive information and clear configuration settings to prevent the disclosure of restricted network information. Where portable hard drives are used, sanitize the disk in accordance with this handbook.

11-11.8.5 Security Requirements for Using a Public Hot Spot

Personnel connecting to public WLANs in airports, hotels, restaurants and such must take the following precautions:

a. Turn off file and print sharing from your wireless device.

b. Clear your list of "preferred networks."

c. Turn off ad hoc networking and ensure your wireless card remains in "infrastructure only" mode.

d. When using a virtual private network to connect back to the Postal Service Intranet, disable split tunneling.

e. Use a personal firewall that detects malicious scanning of your wireless device.

11-11.9 Compliance and Monitoring Requirements

Security assessments and audits are essential tools for checking the security posture of a wireless technology and for determining corrective action to ensure the network remains secure. It is important to perform regular audits using wireless diagnostic hardware and software. Administrators should periodically check for rogue access points and against other unauthorized access.

Only authorized personnel may use diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers).

Dedicated wireless monitoring that performs a full traffic analysis must be implemented to identify wired and wireless security issues and respond appropriately.

12 Service Continuity Plan

12-1 Service Continuity Policy

Service Continuity (SC) consists of the alignment of Business Continuity Plans (including Emergency Action Plans) and Disaster Recover Plans. CIO SC enhances the operational resilience of CIO organizations, their systems, and processes.

The Service Continuity Plan develops the management and governance framework for Postal Service CIO organizations to prepare for, respond to, and recover from any event that disrupts, or threatens to disrupt, normal operations. This policy is applicable to all CIO Service Partners and Owners (see Chapter 2, Security Roles and Responsibilities).

This policy ensures creation of missing plans (including Postal Service Disaster Recovery (DR) Plans, Business Continuity (BC) Plans, Functional (FF) Plans, and Emergency Action Plans (EAP), as well as review of alignment or augmentation of existing plans, by the CIO organizations as defined and mandated elsewhere in this document (Handbook AS-805) and Management Instruction (MI) AS-280-2018-1, *Integrated Emergency Management Supporting Field Business Continuity,* (published January 2018).

This policy, its recommendations, and resulting products (plans) are in compliance with the following:

a. The National Institute of Standards and Technology (NIST) SP 800.34.

b. Homeland Security Exercise and Evaluation Program (HSEEP).

c. Postal Service *Employee Labor Manual* (ELM), 810, Occupational Safety and Health Program; 840, – Safety Awareness Program; and 850, Emergency Action Plans and Fire Prevention and Control.

d. MI AS-280-2018-1, *Integrated Emergency Management Supporting Field Business Continuity.*

Specifically, this policy provides for the: identification, prioritization, vetting, and approval of CIO VP High-Value Services (HVS); compliance with Federal and Postal Service standards and guidelines for recovery plan(s) documentation, maintenance (updating), testing, exercising, and evaluation (TT&E); and personnel training.

The CIO SC policy ensures development of all Postal Service CIO organization's (CIO, Business Services Organization (BSO), Corporate Information Security Office (CISO), Enterprise Analytics (EA), Engineering (ENG), Information Technology (IT), and Mail Entry and Payment Technology (MEPT)) capability to prepare for, respond to, and recover from any event

that disrupts, or threatens to disrupt, normal operations which depend on services provided through the CIO organization. The program improves organizational and technology resilience processes and capabilities to ensure critical CIO services continue during and after an incident and applies to all Postal Service functional organizational elements and personnel.

This is achieved through the establishment and implementation of standards and guidelines for CIO SC including emergency management, service continuity and disaster recovery activities, and standards and plans (operational risk). Its focus is based on the identification and prioritization of the CIO's and VP's high-value services and their recovery/hardening/ resilience through a governance program which ensures maintenance and training on service continuity.

Specifically, through the development, documentation, and implementation of testing, exercising and evaluation processes, and documentation which validate compliance (or noncompliance) to CIO service continuity standards, guidelines, and processes, and effectively address noncompliance and corrective action the developed strategies and plans to sustain functions during a disruption can be practiced.

Service Continuity Management (formerly Business Continuity Management) focuses on resilience. Resiliency is not a process, but rather an end-state for organizations in which the organizations have the ability to quickly adapt and recover from any known or unknown changes to the environment. The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions. Risk management, contingency, and continuity planning are individual security and emergency management activities that can also be implemented in a holistic manner across an organization as components of a resiliency program.

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope; however, because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the following basic descriptions:

a. Business Continuity Plan (BCP) is the documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. *https://csrc.nist.gov/glossary/term/business-continuity-plan*

b. Contingency plan normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

c. Emergency Response (ER) Plan serves as a documented, organized process to manage an unexpected or dangerous occurrence and limit negative impact.

d. Incident Response (IR): IR serves as a documented organized process to manage the aftermath of any incident. The goal is to limit negative consequences of the event.

e. IT Incident Response Plan (IT-IRP) serves as a process to address the aftermath of any technology event or incident and at a minimum includes: Incident Severity definitions, IT IR Procedure, Contact Information and Communications expectations.

f. Cyber Incident Response Plan (C-IRP normally focuses on detection, response, and recovery to a computer security incident or event.

g. Disaster Recovery (DR) Plan defines how work can be resumed after a disaster.

12-2 Service Continuity Plan Requirements

The purpose of business continuity plans are to ensure that business processes which rely upon personnel to perform specific functions will continue after an unplanned emergent event. This event may affect the prerequisite or dependent personnel, tools, or facilities and require that the function be relocated or that an alternate process be initiated.

Business Continuity Plans mitigate operational risk by doing the following:

a. Protecting personnel and identifying essential business processes during an incident or disaster.

b. Reducing the impact of an incident or disaster on facilities' personnel and business processes.

c. Satisfying business continuity needs as defined by USPS management and aligning with industry best practices and United States federal government requirements and guidance.

The minimum requirements for Business Continuity Plans are defined in the following documents:

a. ASM, 28, Emergency Preparedness.

b. Management Instruction (MI) AS-280-2018-1, *Integrated Emergency Management Supporting Field Business Continuity* (published October 24, 2016).

c. Federal Continuity Directive 1 (FCD 1), "Federal Executive Branch National Continuity Program and Requirements" dated January 2017.

All CIO managed facilities will use the structure, tools, products, and nomenclature of the integrated emergency management (IEMM / IEMP) discipline to include the following:

a. Emergency Management Team (EMT) concept of operations.

b. Integrated Emergency Management Module (IEMM) within the Facilities Database System for data entry.

c. Integrated Emergency Management Plan (IEMP) that consists of emergency action, fire prevention, and continuity of operations (COOP) plans, and emergency response checklists.

d. Business Continuity Preparedness (BCP) cyclical requirements for testing, training, exercise, and review.

e. IEMP update and certification requirements.

12-3 Disaster Recovery Plan Requirements

12-3.1 General

All Application and Infrastructure Service owners must develop Disaster Recovery (DR) plans to provide for the resumption of automated systems in the event that those systems are unable to operate as built. Application teams develop Application Disaster Recovery Plans (ADRP). These plans make a reference to dependent Infrastructure Services but recovery of those services is not in scope for the ADRP. Infrastructure Services develop Infrastructure Disaster Recovery Plans (IDRP) that are designed to achieve the RTO (Recovery Time Objective) of the applications that rely on these services.

Both Applications and Information Technology Infrastructure systems need to be designed to achieve availability targets required to sustain the business functions they support. See 9-9 of this document for Availability requirements.

Application and Infrastructure Service owners may use templates when developing DR plans.

12-3.2 Application Disaster Recovery Plan Requirements

The Application Disaster Recovery Plan (ADRP) Requirements are as follows:

a. Each application that is registered in the Enterprise Information Repository (EIR) must have an ADRP.

b. The requirements for the plan are determined based on the Criticality results of the Business Impact Assessment (BIA). See 3-2.3 of this document for requirements of Criticality determination. The ADRP must be designed to achieve the recovery time objectives (RTO) required to meet the business requirements as specified in the BIA.

c. The ADRP does not include the recovery plans for the infrastructure that it's depend upon.

d. The ADRP documentation is stored in the Technical Solution Life Cycle (TSLC) IT Artifact Library systems documentation testing section of the application as a Program-Level Artifacts and is considered "Sensitive".

e. The ADRP must be reviewed, tested, and the results certified by the development organization and the executive sponsor. Evidence of the testing and certification must be kept in the TSLC IT Artifact Library as a Program-Level Artifacts and is considered "Sensitive". Test results are also recorded in the EIR system.

f. ADRP's Critical-High and Critical-Moderate applications must be tested within 180 days of the application going into production and within 180 days of changes which would invalidate previous tests.

g. Applications designated as Critical-High must be tested within 18 months of the last successful test.

h. Applications designated as Critical-Moderate must be tested within 36 months of the last successful test and within 12 months of changes which would invalidate previous tests.

i. Non-Critical (Low) applications are not required to conduct testing of their ADRP. As a result, the application may not be recovered in the event of a site outage. It is recommended that when the BIA is reviewed as required in 6-2 of Handbook AS-805A the criticality classification is carefully considered in light of an extended outage.

j. Failed tests must be re-attempted within 90 days of the failed test.

k. All recovery documents must be protected as restricted information.

12-3.3 Infrastructure Disaster Recovery Plan (IDRP)

Infrastructure Disaster Recovery Plan is an internal documented process or set of procedures to recover and protect the Postal Service IT Infrastructure in the event of a disaster as follows:

a. Many applications are dependent on shared information technology infrastructure services. Therefore these services must be designed to meet the availability requirements of the applications using the service. See 9-9 for availability requirements.

b. The IDRP must support the RTO for the most critical application that uses the Infrastructure Service.

c. The IDRP must be developed and certified by the Infrastructure Service Owner and the executive sponsor (see 2-2.11, Executive Sponsors).

d. The IDRP must be maintained in the designated plan repository. The availability to the repository must not be dependent on any one facility.

e. Infrastructure Services must have contingency plans that address the following:

(1) Loss of capacity due to failures of underlying requirements (power, cooling, facilities, servers, network, etc.).

(2) Loss of connectivity.

(3) Denial of Service attacks.

(4) Data corruption.

f. The IDRP must be exercised quarterly to insure DR infrastructure services provide the same functionality as production.

g. Test activities and results are documented as part of the normal change and configuration management services.

The IDRP must include essential personnel to support and validate recovery.

This page intentionally left blank

13 Security Incident Management

13-1 Policy

Postal Service information resources must be protected against events that may jeopardize information security by contaminating, damaging, or destroying information resources. The Postal Service requires that all information security incidents be immediately reported to CyberSafe regardless of whether damage appears to have been incurred.

Security incident management topics addressed in this chapter include the following:

a. Information security incident identification.

b. Incident prevention, reporting, response, and containment.

c. CyberSafe incident process and activities.

All personnel must adhere to the incident prevention, reporting, and containment standards to ensure adequate protection of Postal Service information resources.

13-2 Information Security Incident Identification

Information security incidents are events, whether suspected or proven, deliberate or inadvertent, that threaten the integrity, availability, or confidentiality of information resources. The reporting of incidents enables the responsible organizations to review the security controls and procedures; establish additional, appropriate corrective measures, if required; and reduce the likelihood of recurrence. To protect the Postal Service computing environment, the manager, Corporate Information Security Office (CISO), may become involved at any point on any level for information security-related incidents impacting the Postal Service.

Reportable incidents include, but are not limited to, the following:

a. Physical loss, theft, or unauthorized destruction of Postal Service information resources (e.g., missing or damaged hardware, software, or electronic media).

b. Unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information.

c. Internal or external unauthorized access attempts to access information or the facility where the information resides.

d. Unauthorized activity or transmissions using Postal Service information resources.

e. Internal or external intrusions or interference with Postal Service networks (e.g., denial-of-service attacks, unauthorized activity on restricted systems, unauthorized modification or deletion of files, or unauthorized attempts to control information resources).

f. Information resources with system software that is not patched to the current level.

g. Information resources with virus protection software that is not patched to the current level or is disabled.

h. Information resources with virus pattern recognition files that are not current.

i. Sudden unavailability of files or data normally accessible.

j. Unexpected processes (e.g., e-mail transmissions) that start without user input).

k. Files being modified when no changes in the files should have occurred.

l. Files appearing, disappearing, or undergoing significant and unexpected changes in size.

m. Systems displaying strange messages or mislabeled files or directories.

n. Systems becoming slow, unstable, or inaccessible (e.g., will not boot properly).

o. Data altered or destroyed or access denied outside of normal business procedures.

p. Detection of unauthorized personnel in controlled information security areas.

q. Security violation, suspicious actions, or suspicion or occurrence of embezzlement or other fraudulent activities.

r. Suspected bribery, kickbacks, and conflicts of interest.

s. Revenue loss involving an information system.

t. Prohibited mass electronic mailings.

u. Potentially dangerous activities or conditions.

v. Illegal activities.

w. Violation of Postal Service information security policies and procedures.

x. Identity theft.

y. Detection of unauthorized wireless access points.

13-3 Incident Prevention, Reporting, Response, and Containment

13-3.1 Incident Prevention

The following actions by Postal Service personnel can help prevent information security incidents:

a. Display proper badge when in any Postal Service facility.

b. Be aware of your physical surroundings, including weaknesses in physical security and the presence of any unauthorized visitor.

c. Use only approved computer hardware and software with the latest patches installed.

d. Use updated virus protection software and pattern recognition files.

e. Do not download, install, or run a program unless you know it to be authored by a person or company that you trust.

f. Use a personal firewall.

g. Use a strong password of at least eight characters composed of upper- and lower-case alphabetic, numeric, and special characters.

h. Encrypt sensitive-enhanced and sensitive information physically removed from a Postal Service facility.

i. Encrypt sensitive-enhanced and sensitive information in transit.

j. Back up data stored on local workstation and physically secure the backup copies.

k. Be wary of unexpected attachments. Know the source of the attachment before opening it. Remember that many viruses originate from a familiar e-mail address.

l. Be wary of URLs in e-mail or instant messages. A common social engineering technique known as phishing uses misleading URLs to entice users to visit malicious Web sites. URLs can link to malicious content that, in some cases, may be executed without your intervention.

m. Be wary of social engineering attempts to solicit sensitive-enhanced or sensitive information (e.g., account numbers and passwords).

n. Users of technology such as instant messaging and file-sharing services should be careful of following links or running software sent by other users.

13-3.2 Incident Reporting

Information security incidents must be immediately reported to CyberSafe via telephone at 1-800-USPS-HELP or via an e-mail to *CyberSafe@usps.gov*. The CyberSafe telephone number is a 24 X 7 hotline. Do not dismiss a suspected incident or discount its seriousness.

In addition to CyberSafe, the following personnel may be notified, as appropriate:

a. Help Desk at 1-800-USPS-HELP or 1-800-877-7435.

b. Immediate supervisor or manager.

c. Local system administrator or local technical support.

d. Security control officer (SCO).

e. Inspection Service at 1-877-876-2455.

f. Office of the Inspector General (OIG) at 1-888-877-7644.

A PS Form 1360, *Information Security Incident Report,* must be completed and submitted to CyberSafe. An acceptable facsimile with the same information required on the form may be submitted.

13-3.3 Incident Response

Information security situations and incidents must be handled in a way that minimizes damage, reduces recovery time and costs, and mitigates the risks to our customers and personnel. CyberSafe coordinates responses to information security situations and incidents.

13-3.4 Incident Containment

When an information security-related situation or incident is suspected or discovered, personnel must take steps, as directed by CyberSafe, to protect the information resource(s) at risk. Appropriate actions are the following:

a. Do not shut down or power off a system after a computer incident occurs. All suspect systems and devices that are already powered down should remain in that state.

b. Do not make any changes to the equipment or network in question without direction from CyberSafe.

c. Do not discuss or e-mail anyone about the situation or incident unless directed to do so by CyberSafe.

d. Follow CyberSafe instructions with regard to options and strategies for containment and recovery from the incident.

e. Close and lock doors to protect unattended equipment.

f. Do not touch the keyboard. Take a photograph of the screen or make a note of the information displayed before turning off the computer monitor so the screen cannot be viewed.

g. Challenge personnel without badges.

Supervisors or managers who suspect, discover, or are notified of a security-related event must initiate the following response procedures to contain the incident, protect the confidentiality and integrity of Postal Service information, and ensure business continuity:

a. Notify CyberSafe for assistance to contain, eradicate, and recover from the security incident.

b. Notify the Inspection Service of a physical security incident.

c. Document in a journal or log all conversations and actions taken during the incident handling and response process and make this log available to management personnel on request.

d. Ensure personnel follow contingency plans for recovering from disruptive incidents.

e. Ensure the completion of a PS Form 1360.

13-3.5 Mass Data Compromise Plan

Implement a Mass Data Compromise Plan (MDCP) to provide a strategy for addressing the dynamics of a critical incident. A critical incident is one that threatens confidentiality, integrity or availability of Postal Service information assets with high impact, high threat involving high risk and great vulnerability. The MDCP defines the roles and responsibilities for critical incident response team members, defines critical incident severity levels, outlines a process flow for critical incident management, and includes methodologies for conducting response activities.

13-4 CyberSafe Incident Process and Activities

13-4.1 Preliminary CyberSafe Activities

The following preliminary activities can improve CyberSafe's ability to respond to information security incidents:

a. Develop an incident response plan. Predetermine necessary actions and responses to specific classes of incidents to facilitate making decisions under pressure with minimal information.

b. Implement secure connections to make intrusion detection system (IDS) policy changes and attack signature updates.

c. Verify automated responses from IDS.

d. Conduct penetration testing at times known only to personnel with a need to know.

e. Regularly review available information sources (e.g., advisories and research findings) to maintain currency.

f. Notify management of potentially harmful events.

g. Prioritize the severity of information security incidents.

h. Document lessons learned to improve CyberSafe operations.

13-4.2 CyberSafe Incident Process

13-4.2.1 Incident Categorization

Incidents must be categorized based on severity and associated response times. The severity of the incident will determine the appropriate notification process and escalation procedure. Incident severity levels and response times are defined as follows (per the Postal Service CyberSafe severity code procedures):

a. Severity 1 — National Impact: Incidents with the greatest negative impact on the Postal Service. Severity level 1 is assigned when an incident has national impact or when multiple systems or sites are down or seriously affected.

b. Severity 2— Site Impact: Incidents impacting a major IT or field site or local area network (LAN) segment.

c. Severity 3 — Customer Impact: Incidents impacting one or more workstations, employees, contractors, or customers.

d. Severity 4 — Minimal Impact: Incidents with minimal or no impact.

13-4.2.2 Processing Incidents Reports

CyberSafe is responsible for the following:

a. Categorizing incidents.

b. Protecting the confidentiality of information contained in the incident report and subsequent information identified in the analysis.

c. Ensuring legal issues, requirements, and restraints caused by criminal and civil investigations are appropriated addressed.

d. Logging and tracking security incident reports.

e. Monitoring incidents to ensure appropriate response and immediate resolution of security incidents.

f. Engaging appropriate organizational resources (e.g., virus response team, OIG, and Inspection Service).

g. Notifying the CPO and responsible functional VP (data steward) of any suspected breaches involving sensitive or sensitive-enhanced information.

h. Evaluating and escalating incident reports requiring further action.

i. Retaining incident reports, supporting evidence, and journals for 1 year or for a time period determined by the OIG.

j. Providing Inspection Service and OIG access to all reported information security incidents.

k. Complying with federal sector security incident reporting requirements.

13-4.2.3 Incident Investigation

A member of the OIG-CCU team is co-resident with CyberSafe and investigates, along with the Inspection Service, violations of state and federal laws enacted to protect the authenticity, privacy, integrity, and availability of electronically stored and transmitted information.

13-4.2.4 Incident Analysis

CyberSafe analyzes security incidents and prepares reports summarizing the causes, frequency, and damage assessments of information security incidents.

CyberSafe management analyzes CyberSafe reports to improve the information security program and keep Postal Service executive management apprised on the state of information security.

13-4.2.5 Incident Escalation

It may be necessary to escalate an individual incident up the management chain based on the following criteria:

a. Number of sites and systems under attack.

b. Type of data at risk.

c. Severity of the attack.

d. State of the attack.

e. Source or target of the attack.

f. Impact on the integrity of the infrastructure or cost of recovery.

g. Attack on a seemingly "secure" information resource.

h. Personnel awareness of the attack.

i. New attack method use.

13-4.2.6 Incident Closure

Before an incident is closed the incident must be categorized; the root cause must be determined; damage must be assessed and reported to management and one or more of the national CyberSafe if required; and the incident's closure confirmed with the initiator.

14 Security Compliance and Monitoring

14-1 Policy

All Postal Service information resources are the property of the Postal Service. The Postal Service has the legal right to monitor and audit the use of its information resources as necessary for compliance with policies, processes, procedures, and standards to ensure the appropriate use and protection of Postal Service information resources.

The activities of all Postal Service personnel who use Postal Service computing resources may be subject to audit or monitoring, and any detected misuse of Postal Service computing resources may be subject to disciplinary action up to and including removal, termination, and criminal prosecution.

Security topics addressed in this chapter include the following:

a. Compliance.

b. Monitoring.

c. Audits.

d. Confiscation and removal of information resources.

This monitoring policy does not apply to Postal Service customers who visit the Postal Service Web site (i.e., no attempt is made to identify individual customers or their usage habits). See the Postal Service Privacy Policy on *http://www.usps.com* for additional information.

14-2 Compliance

The Postal Service exercises due care in ensuring all personnel and contractors working on its behalf are in compliance with information security policies and associated standards and procedures as defined by the Postal Service. Additionally, the Postal Service monitors, reviews, and properly mitigates all instances of noncompliance throughout the organization using processes that include, but are not limited to, the following:

a. Regular testing of security systems and processes.

b. Vulnerability scans.

c. Inspections, reviews, and evaluations.

d. Monitoring.

e. Audits.

f. Confiscation and removal of information resources.

g. Information security compliance training.

The importance of compliance with government and industry regulations and standards is to prevent data breaches, loss of reputation and customers, fines and lawsuits.

14-2.1 Regular Testing of Security Systems and Processes

Systems, processes, and custom software must be tested regularly because hackers and others continually discover vulnerabilities introduced in new software inadvertently by employees, contractors, and business partners. How testing is conducted is described in Exhibit 14-2.1.

Security testing must replicate real world attacks to [1] determine the effectiveness of preventive controls and if critical assets are exposed and [2] to provide insight into the actual risk posture of the information resource and highlight trends.

Exhibit 14-2.1

Regular Testing of Security Systems and Processes

Frequency	Testing Activities
Continuously	Monitor all network traffic and alert personnel to suspected compromises using network intrusion-detection systems, host-based intrusion detection systems, and intrusion prevention systems.
Weekly	Use file integrity monitoring software to alert personnel when files have been modified without authorization. Configure software so it can compare files.
Quarterly	Use a wireless analyzer to identify all wireless devices in use. Scan for vulnerabilities in internal and external networks (or when system components have been added, network topology has changed, firewall rules have been modified, or products have been updated).
Annually	Test security controls, limitations, network connections, and restrictions to identify unauthorized access attempts. Perform network-layer penetration testing (or when the infrastructure has been upgraded or modified (i.e., the operating system has been upgraded or a subnetwork or Web server has been added). Perform application-layer penetration testing (or when an application has been modified) to understand the intricate interactions and exploitable paths hidden in the code.
As Required	Whenever changes are made to the PCI environment. Whenever the Hardening Standards Team requests a hardening standards compliance check to ensure Postal Service hardening standards are being implemented.

The risks associated with newly discovered vulnerabilities must be documented and forwarded to the Corporate Information Security Office/ ISSO for inclusion into either the Risk Mitigation Plan for each system or Risk Register.

14-2.2 Vulnerability Scans

The Corporate Information Security Office Information Systems Security (CISO ISS) conducts vulnerability scans on applications, infrastructure components, and facilities. The vulnerability scan process identifies and assigns a risk ranking to security vulnerabilities based on industry best practices. For example, a "High" risk vulnerability will include a CVSS base score of 4.0 and above, and/or a vendor-supplied patch missing that is classified as "critical" and/or a vulnerability affecting a critical system component. The executive sponsor is responsible for coordinating the resolution of the vulnerabilities identified with the responsible organization (e.g., the manager IT Computer Operations for operating system and database software; the Business Relationship Management manager for application software, etc.).

14-2.3 Inspections, Reviews, and Evaluations

Inspections, reviews, and evaluations must be conducted for information resources and facilities to ensure compliance with Postal Service information security policies. A process is in place to monitor internal control compliance on an ongoing basis.

The CISO conducts inspections, reviews, and evaluations of information resources:

a. As part of the certification and accreditation (C&A) process.

b. When informally or formally requested by the supervisor or manager of an information resource.

c. At the discretion of the CISO or the VP IT Operations as necessary to evaluate the security of information resources.

The Inspection Service and/or CISO conducts inspections, reviews, and evaluations of Postal Service facilities.

14-2.4 Penetration Testing

The Corporate Information Security Office Cybersecurity Risk Penetration Testers conduct penetration testing on applications, infrastructure components, and facilities. Although USPS leaders and Information System managers are expected to engage in scheduled penetration testing engagements, such as those prescribed elsewhere within this document, CISO Risk reserves the right to perform penetration testing as needed throughout the organization.

Postal personnel are expected to provide assistance as directed by the needs of the penetration testers in the course of their assessment activities, to include disclosure of documentation and access to perform testing. Engagements may be performed as needed at the direction of the CISO and Cybersecurity Risk Managers to provide independent validation, assist in investigations, and to help audit processes and procedures throughout The Postal Service.

14-3 Monitoring

Monitoring is used to improve security for Postal Service information resources to ensure appropriate use of those resources and to protect Postal Service resources from attack. Use of Postal Service information resources constitutes permission to monitor that use. Nonbusiness (i.e., personal) information may be viewed when monitoring Postal Service information resources.

All personnel are advised that the information on Postal Service non-publicly available information resources may be monitored and viewed by appropriate, authorized personnel, regardless of privacy concerns. The Postal Service reserves the right to do the following:

a. Review the information contained in or traversing Postal Service information resources.

b. Review the activities on such information resources.

c. Act on information discovered as a result of monitoring and disclose this information to law enforcement and other organizations as deemed appropriate by Postal Service personnel.

14-3.1 What Is Monitored

Monitoring of Postal Service information resources may include, but is not limited to, the following:

a. Network traffic.

b. Application and data access.

c. Keystrokes and user commands.

d. E-mail and Internet usage.

e. Message and data content.

f. Unauthorized access points.

14-3.2 User Agreement to Monitoring

Any use of Postal Service information resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of Postal Service information resources:

a. Agree to comply with Postal Service policy concerning the use of information resources.

b. Acknowledge that their activities may be subject to monitoring.

c. Acknowledge that any detected misuse of Postal Service information resources may be subject to disciplinary action and prosecution pursuant to the United States Criminal Code (Title 18 U.S.C. § 1030).

14-3.3 User Monitoring Notification

Where possible, users are notified by the display of an authorized Postal Service warning banner (see Exhibit 14-3.3) that the information on Postal Service networks and workstations may be monitored and viewed by authorized personnel, regardless of privacy concerns.

The Postal Service-authorized warning banner must be displayed to users prior to granting session access to Postal Service information resources and be included in information security awareness training. The legal authority and obligations as indicated in the warning banner will apply throughout the entire session users have on the Postal Service information resources.

Applications that are single sign-on (SSO) or single log-on (SLO) compliant are not required to display an additional warning banner page as long as the executive sponsor can guarantee the user will see a warning banner at login for the session. Applications that are not SSO or SLO compliant must display a warning banner page.

Internal warning banners are not intended for display on Postal Service externally facing Internet Web sites where the Postal Service Internet Privacy Policy applies.

At a minimum, the warning banner must accomplish the following:

a. Identify the computer system as a Postal Service computer system protected by the United States Criminal Code.

b. Provide notification of monitoring.

c. Be followed by a pause requiring manual intervention to continue.

d. Identify the information resource as a Postal Service information resource and alert users that they have no expectation of privacy.

e. Warn users that activities may be monitored and that unauthorized access is prosecutable pursuant to the United States Criminal Code (Title 18 U.S.C. § 1030).

Note: Deviations from the authorized standard warning banner are not allowed unless approved in writing by the manager, CISO.

Exhibit 14-3.3
Authorized Standard Postal Service Warning Banner

WARNING! FOR OFFICIAL USE ONLY...

This is a U.S. Government computer system or mobile device and is intended for official and other authorized use only. Unauthorized access or use of this system or mobile device may subject violators to administrative action, civil, and/or criminal prosecution under the United States Criminal Code (Title 18 U.S.C. § 1030).

All information on this computer system or mobile device to include GPS location services may be monitored, intercepted, recorded, read, copied, captured, and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy using this system or mobile device. Any authorized or unauthorized use of this computer system or mobile device signifies consent to and compliance with Postal Service policies and these terms.

I agree.

14-3.4 Requesting User Monitoring

Requests for monitoring network traffic, application and data access, keystrokes and user commands, and e-mail and Internet usage must be in writing and directed to the manager, CISO.

Requests for monitoring message data content or Internet usage must be in writing and directed to the chief privacy officer (CPO).

14-3.5 Approving User Monitoring

The manager, CISO, has the responsibility to authorize in writing monitoring or scanning activities for network traffic, application and data access, keystrokes and user commands, and e-mail and Internet usage for Postal Service infrastructure or information resources. Personnel (except the Inspection Service and OIG) must receive authorization from the CISO prior to conducting monitoring and scanning activities.

The CPO has the responsibility to authorize, in writing, requests for message data content, or Internet usage monitoring. The Information Catalog Program (ICP) Office is responsible for documenting and servicing the request.

In case of threats to the Postal Service infrastructure, network, or operations, the manager, CISO, is authorized to take appropriate action, which may include viewing and/or disclosing data to protect Postal Service resources or the nation's communications infrastructure.

14-3.6 Infrastructure Monitoring

The manager, CISO, is responsible for ensuring the security of the Postal Service infrastructure through the following:

a. Providing security incident detection through perimeter virus scanning, intrusion-detection services, and security event correlation tools.

b. Performing network, Web, host, application, and database vulnerability analyses.

c. Performing data loss prevention analyses to prevent sensitive and sensitive-enhanced information from leaving the protected environment.

d. Performing data at rest searches for unprotected sensitive and sensitive-enhanced information.

e. Monitoring the Postal Service infrastructure, investigating incidents, and resolving or reassigning incidents immediately to the appropriate group for action.

f. Monitoring system-level audit logging.

g. Monitoring PCI service providers for compliance with the current PCI DSS.

14-3.7 Intrusion Detection

Intrusion-detection devices are implemented to monitor the infrastructure. The use of all monitoring devices, except those used by the OIG, must be approved by the manager, CISO ISS. Unauthorized installation and use of monitoring devices are strictly prohibited.

14-3.8 Data Loss Protection Program

The Data Loss Protection (DLP) program was implemented to protect sensitive and proprietary information entrusted to the Postal Service by its employees, customers, contractors, and vendors (suppliers). The DLP program supports Postal Service compliance with the Privacy Act, the PCI industry, many state identity theft notification laws, the Gramm-Leach-Bliley (GLB) Act, and the Sarbanes Oxley (SOX) Act. The software-based solution uses business rules to analyze the contents of all outbound electronic communications including email, web mail, file transfers, other web-based (HTTP) messages to look for sensitive information. The current business rules look for the existence of credit card numbers and social security numbers being transmitted in clear text. When sensitive information is found, the message is flagged for further analysis by CISO.

14-3.9 Continuous Monitoring Guidelines

To ensure compliance with information security policies, the Postal Service must regularly assess its information security readiness and implement

solutions that mitigate vulnerabilities, misconfigurations, and prevent unnecessary exposures by providing real-time visibility and control over servers, desktops, laptops, notebooks, and other mobile devices.

Given that threats are constantly evolving, the Postal Service must monitor critical assets more frequently so they can detect if something illegal or unauthorized has occurred and respond quickly to minimize the damage.

The most important actions/assets to monitor continuously are the ones that are most volatile (e.g., new versions of software and new hardware) and the ones the attackers are exploiting. The Consensus Audit Guidelines (were developed to address the continuous monitoring requirements delineated in National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

The Consensus Audit Guidelines recommended frequencies for meeting the requirement for continuous monitoring are:

a. Test the computing environment, including servers and workstations, three times a day.

b. Check for vulnerabilities at least once a week.

c. Check configuration settings no less than once every 15 days.

For example, the Department of Homeland Security Continuous Diagnostics and Mitigation program goal is to scan critical systems every 20 minutes (all systems every 1 to 3 days), collect results, triage and analyze results, and fix the worst problems first.

The Postal Service must understand the day-to-day operational status of controls deployed and how those controls are standing up to cyber threats.

Areas of focus must be hardware and software asset management, configuration settings, account and privilege management, ports/protocols/ services for infrastructure devices, local computing environment events, network and infrastructure events, and enclave events.

14-4 Audits

14-4.1 Conducting Audits

The OIG has the authority to conduct audits, investigations, and evaluations of Postal Service programs and operations to ensure the efficiency and integrity of the Postal Service. The OIG coordinates investigative audits through the manager, CISO. Audits associated with financials [e.g., year-end audits and Sarbanes-Oxley Act (SOX) audits] are coordinated through the SOX Program Management Office.

14-4.2 Responding to Audits

Corporate management responsible for the audited information resource must respond to internal and external audit findings and ensure that the information resources under their control comply with Postal Service information security policies and procedures.

14-4.3 Audit Guidelines

The following critical information security controls identified in the CAG represent the highest-priority defenses that the Postal Service should focus on, based on the likelihood of real-world attacks:

a. Inventory of authorized and unauthorized devices.

b. Inventory of authorized and unauthorized software.

c. Secure configurations for hardware and software on laptops, workstations, and servers.

d. Secure configurations for network devices including firewalls, routers, and switches.

e. Boundary defense.

f. Maintenance, monitoring, and analysis of security audit logs.

g. Application software security.

h. Controlled use of administrative privileges.

i. Controlled access based on need to know.

j. Continuous vulnerability assessment and remediation.

k. Account monitoring and control.

l. Malware defenses.

m. Limitation and control of network ports, protocols, and services.

n. Wireless device control.

o. Data loss prevention.

p. Secure network engineering.

q. Penetration tests.

r. Incident response capability.

s. Data recovery capability.

t. Security skills assessment and appropriate training to fill gaps.

14-5 Confiscation and Removal of Information Resources

The CISO, OIG, Inspection Service, or their designee may confiscate and remove any information resource suspected to be the object of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be used in forensic analysis of a security incident. The CISO, OIG, Inspection Service, or their designee, as appropriate, must verify that the chain of evidence (associated with the possession of the confiscated information resource) is preserved and documented.