LABOR RELATIONS

UNITED STATES POSTAL SERVICE

March 9, 2020

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

Dear Brian:

As a matter of general interest, the Postal Service is revising Handbook AS-805, *Information Security*, Section 6-6, *Departing Personnel*; Section 9-4, *Accountability*; and Section 9-5, *Identification*.

The main purpose of the revisions is to establish that employee eAccess accounts will be suspended in situations in which an employee remains, or is expected to remain, in a Leave Without Pay status for a period in excess of calendar 30 days. Under these circumstances, the employee's supervisor may reactivate the eAccess account upon the employee's return to work. Additionally, the revisions establish that any account that is unused for 30 calendar days will be suspended until such time that it is reactivated by the employee's supervisor.

We have enclosed two copies of the subject revisions, one with and one without changes identified.

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

Sincerely,

David E. Mills
A/Manager
Labor Relations Policies and Programs

Enclosures

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

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 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 employees, 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 of an individual being terminated under adverse circumstances must do the following:
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.

For 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 and 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 contractor's/supplier's eAccess account is terminated.
g. Before escorting the individual off the premises, secure the Postal Service badge/ID.

9-4 Accountability

9-4.3 Account Management

Internal Accounts – Accounts must be established in a manner that ensures access is granted based on clearances, needed to know, separation of duties, and least privilege basis. Accounts unused for 30 days must be disabled. Accounts unused for 1 year must be deleted.

External users (customer 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.

9-5.3 Suspending Log-on IDs

Internal Accounts – After six unsuccessful attempts to log on to an information resource, the log-on ID or account must be suspended 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 followed defined procedures for resolution.

Employees who remain in a Leave Without Pay (LWOP) status for a period in excess of 30 days, or who are expected to be in a LWOP status in excess of 30 days, must have their eAccess account suspended 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 – For externally facing login pages, do as follows,

a. After 5 successful 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.
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.

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 employees, ~~T~~the ~~individual's~~ employee computer log-on ID, building-access authorizations, and access to Postal Service information systems are terminated coincident with the employee's ~~or contractor's~~ effective date of departure determined by Human Resources, unless needed in the new assignment.

~~b.~~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.

~~c.~~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 do the following:

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.

For 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 and 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 contractor's/supplier's eAccess account is terminated.
g. Before escorting the individual off the premises, secure the Postal Service badge/ID.

9-4 Accountability

9-4.3 Account Management

Internal Accounts – Accounts must be established in a manner that ensures access is granted based on clearances, needed to know, separation of duties, and least privilege basis. Accounts unused for ~~90~~30 days must be disabled. Accounts unused for 1 year must be deleted.

External users (customer 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.

9-5.3 Suspending Log-on IDs

Internal Accounts – After six unsuccessful attempts to log on to an information resource, the log-on ID or account must be suspended 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 followed 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 30 days, or who are expected to be in a LWOP status in excess of 30 days, must have their eAccess account suspended 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 – For externally facing login pages, do as follows,

a. After 5 successful 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.
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.