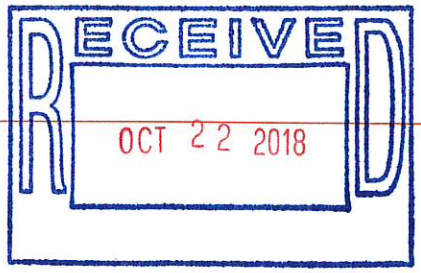
LABOR RELATIONS

UNITED STATES
POSTAL SERVICE



October 16, 2018

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

Dear Brian:

This is in further reference to our October 4 correspondence concerning revisions to Handbook AS-805, *Information Security*.

Additional edits have been incorporated into the final draft. We have enclosed a copy of these edits, which are found in Section 5-5, *Prohibited Use of Information Resources*.

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

Sincerely,

Alan S. Moore
Manager
Labor Relations Policies and Programs

Enclosure

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

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, ~~decrypt~~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 ~~discredit,~~ defame, libel, ~~abuse, embarrass, tarnish, present a bad image of, or portray in false light~~ 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 connection of Postal Service-sponsored cell phones to the Postal Service intranet (Blue) or Postal Service computing devices, regardless of purpose, is unauthorized. The physical or wireless connection of other Postal Service peripheral devices or personal peripheral devices to the Postal Service intranet (Blue) or Postal Service computing devices 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.*