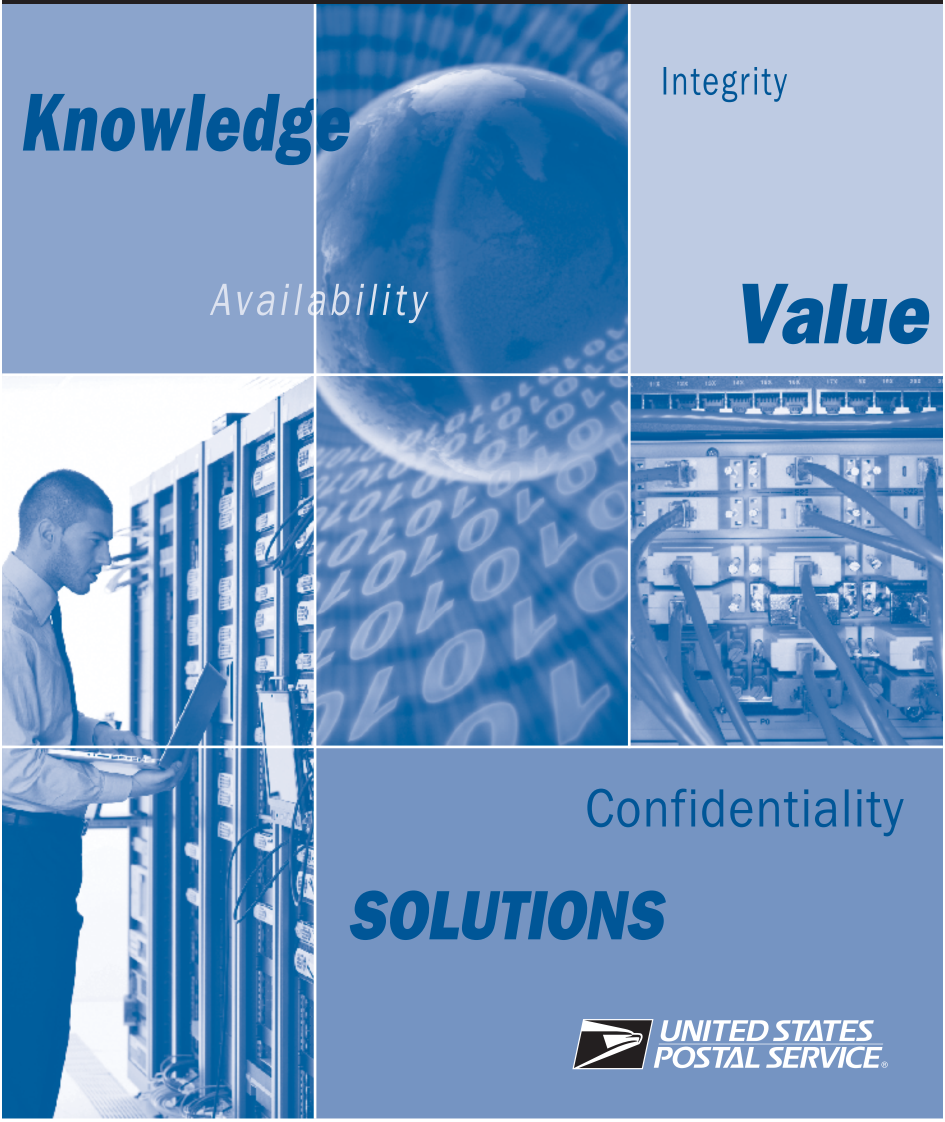
INFORMATION TECHNOLOGY
Value | Knowledge | Technology

Information Security for General Users



UNITED STATES
POSTAL SERVICE®

June 2013

POSTAL SERVICE INFORMATION TECHNOLOGY USERS

SUBJECT: Information Security Resources

This handbook summarizes what you need to know about using Postal Service™ information resources and the information security policies that govern their use.

Your appropriate use of the resources that the Postal Service provides is important. It can affect the efficiency of our day-to-day business activities, the success of new business opportunities, and the preservation of the trust and security represented by the Postal Service brand.

By knowing and carrying out your responsibilities, you become a major contributor to a successful information security strategy.

Take time to understand the significance of your role. If you have questions and can't find the answers in this document, call our Information Security Services Office at 919-501-9350. We want to help you help us.

When you understand your role and responsibilities in protecting Postal Service information, follow the instructions on the last page of this handbook to provide an acknowledgement to your manager.

Ellis A. Burgoyne
Chief Information Officer
and Executive Vice President/Acting

Contents

1. Introduction

What This Handbook Covers

HBK AS-805
Available at *http://about.usps.com/handbooks/as805c.pdf*

This handbook summarizes information security policies for general users of Postal Service information resources. For a complete explanation of information security policies, please refer to HBK AS-805, *Information Security.*

2. Logon IDs, Passwords, PINs, and Tokens

Temporary Information Services
Active directory account, e-mail, office suite of services, and intranet browser access.

eAccess
Online computer request application at *https://eaccess.usps.gov.*

Logon ID
A unique identifier assigned to a user when access is authorized.

Getting Access

The Postal Service uses logon identifications (IDs), passwords, personal identification numbers (PINS), and tokens to manage access to its information resources.

Need access to basic computer services?

If you don’t have access to computer services but need it to do your job, use eAccess to ask your supervisor or manager. Information Technology will notify you when you have been granted access to computer services.

Need additional access?

If you already have access to basic computer services but need to add services, then you or your manager can request it using eAccess.

Creating a Password

What to do when you create a password…

Password
A string of characters you 'know' that can be used for authentication, i.e., provides proof that you are who you say you are when using a given logon ID.

- Use alphanumeric passwords with at least eight characters.
- Choose a password that is hard for others to guess, such as phrases or word strings.
- Use at least one character from three of the four following types of characters:
  - Upper case letters (A–Z).
  - Lower case letters (a–z).
  - Numerals (0–9).
  - Non alphanumeric characters (special characters such as &, #, and $).
- Change your password every 90 days.
- See Handbook AS-805 if you are a privileged user or work in Information Technology.

What not to do when you create a password…

- Do not use all the same characters or digits or other commonly used or easily guessed formats.
- Do not use your name, family members' names, birth date, or other personal information.
- Do not use terms such as *Post Office*™ or *user* or other Postal Service terminology or acronyms.
- Do not use words that appear in the dictionary.
- Do not use your logon ID.
- Do not repeat your passwords for at least 5 generations.

Using Logon IDs and Password

What to do when using logon IDs and passwords…

- Keep your password confidential. You are accountable for the actions of anyone using your logon ID and password, even if you didn't give the user permission.
- Change your password if you think it has been compromised.
- If you have forgotten your password or your account has been disabled because you made six unsuccessful attempts to enter your account, use ePassword Reset to

re-set your password. The ePassword Reset program will automatically re-set the password to a temporary password, which you must change the next time you log on to the network.

- If you write your password down, store it under your personal control or in tamper-resistant manner (e.g., an envelope with a registry seal, time stamped, and signed) to ensure that any disclosure or removal of the written password is clearly recognizable.

What not to do when using logon IDs and passwords…

- Do not write your password on a sticky and attach it to your monitor.
- Don't share your password under any circumstances, including in the following examples:
  - Don't share your password with IT technical support staff working to resolve a Help Desk or system upgrade ticket related to your system.
  - Don't share your password with coworkers to enable them to access your system for any reason, e.g., to resolve any issues related to teleworking and to enable them to access a file, application, e-mail message, attachment, or meeting/calendar-related information.
  - Don't share your password with a family member or personal acquaintance to enable them to access the Internet or use MS Office or other USPS® applications installed on a USPS® computing device.
- Never let anyone use your logon ID or password and do not use anyone else's.
- Do not store your password in application code, files, or tables.
- Do not transmit a password for access to your system, to an encrypted document, or to an archive in clear text in an e-mail.

Screensaver
Protects information when you are away from the computer but not logged out.

Using Screensaver Time-Out and Password

- Make sure your screensaver time-out feature is working; and if not, contact the IT Help Desk.

PIN
A specialized authenticator for limited applications and usually used with a token.

Using PINs

- Protect PINs as you protect passwords.

Using Tokens

Token
A small tangible object that contains a built-in microprocessor used to store and process information for authentication.

- Protect your token from theft.
- Do not allow anyone else to use it.
- Do not leave tokens out in plain sight when not in use; secure them in locked drawers.

Resetting Passwords

- If you suspect your password has been compromised, change it immediately by using the Change Password function button on the Window Security Web page (available by simultaneously depressing the *Ctrl, Alt,* and *Delete* keys).
- If you forget your password, use ePassword Reset (available from the Postal Service Intranet, *http://blue.usps.gov,* and from the following links) to reset it:
  - Application Password (*https://epasswordreset.usps.gov*).
  - Mainframe Password (https://epasswordreset.usps.gov).

3. Use of Information Resources

General Use

What to do when using information resources…

Limited Personal Use
See HBK AS-805, Chapter 5, and MI EL-660-2009-10, *Limited Personal Use of Government Office Equipment and Information Technology.*

- Follow Postal Service limited-personal-use policies.
- Protect our workstations, laptop computers, and handheld devices, both on and off Postal Service premises, against theft and misuse by following all Postal Service information security requirements.
- Connect to the intranet weekly to receive appropriate software updates and virus pattern recognition files.
- Use only software on the official list of approved software, which is on the Infrastructure Technology Kit site (ITK) at *http://itk.* Click on Access ITK on the right-hand side. The link will show a list of approved software.
- Obtain your vice president or designee's written approval to use Bluetooth devices on Postal Service premises because of the potential interference to Postal Service systems such as Surface Visibility (SV) and Yard Management (YM).

- Obtain your vice president or designee’s written approval to use personal information resources [e.g., laptops, notebooks, personal digital assistants (PDAs), hand-held computers, or storage media including universal serial bus (USB) devices] on Postal Service premises.
- Use Postal Service-approved encryption software to encrypt sensitive information [e.g., personally identifiable information (PII) and payment cardholder information (PCI)] in transit and at rest and give management recovery keys and decryption instructions.

What not to do when using information resources…

- Do not jeopardize Postal Service information security or impair performance of computer resources.
- Do not attempt unauthorized entry to any computer system.
- Do not install unauthorized hardware or software.
- Do not copy or browse someone else’s personal files or accounts.
- Do not copy, move, or store electronic files containing nonpublic information to local hard drives, removable media, or remote access technologies not related to your normal business activities without written management approval.
- Do not send or store credit or debit card numbers or related cardholder information if not a part of your job responsibilities.
- Do not perform unofficial activities that could degrade the performance of Postal Service equipment or systems, such as playing electronic games and non-Postal Service video files.
- Do not use Postal Service resources to promote or maintain a personal or private business or commit fraudulent or illegal activities.
- Do not use personal information resources (e.g., laptops, notebooks, PDAs, hand-held computers, or storage media including USB devices) at retail counter areas, mail processing areas, or workroom floors; this includes headsets or earpieces attached to such devices. This requirement does not apply to personal information resources used by the unions in accordance with the collective bargaining agreement.
- Do not use cell-phone cameras or retail lobby web-cams

in any manner not authorized by Postal Service MI AS-882-2011-6, Postal Service Use of Retail and *Cell Phone Cameras*.

- Do not connect personal electronic devices to the Postal Service intranet.
- Do not use imaging devices (e.g., cameras, cell phones with cameras, or watches with cameras) at Postal Service facilities, except as authorized by your vice president or someone designated to make business decisions on the vice president's behalf.
- Do not use Bluetooth devices on Postal Service facilities without approval from the user's vice president or designee because of the potential for interference to Postal Systems such as Surface Visibility (SV) and Yard Management (YM).
- Do not disable your password or token-protected screen saver.
- Do not disable your virus protection software.

E-mail Use

What to do when you use e-mail…

Restricted Information Label indicating that access to records or information is restricted based on Postal Service policies.

- You may use Postal Service e-mail for limited personal use only if it doesn't interfere with Postal Service business (e.g., if the activity is of limited duration, messages are of limited size, have a small transmission impact, and require only a small amount of storage and paper, if printed) and does not violate Postal Service policies.
- Send sensitive information and non-publicly available information only to authorized personnel with a Postal Service business-related "need-to-know."
- Use Postal Service-approved encryption software to encrypt sensitive information [e.g., PII and PCI cardholder information] sent by e-mail and give the recipient the recovery keys and decryption instructions.

What not to do when you use e-mail…

Privacy? Don't expect it. E-mail and Internet use may be monitored.

- Never use Postal Service computing devices, including Blackberries, to check your non-Postal Service or personal e-mail accounts or social media pages.
- Do not open an e-mail message from someone you do not know or recognize as a valid business contact.
- Do not open unsolicited or suspicious e-mail attachments.

- Do not click on links in e-mails unless the e-mail is from someone you know or recognize as a valid business contact.
- Do not send information that violates state or federal laws and Postal Service regulations or that could defame, libel, abuse, embarrass, tarnish, or present a bad image of or falsely portray the Postal Service, recipient, sender, or anyone else.

Spam
Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple addresses.

- Do not send or respond to spam. Delete the spam without opening it.
- Do not view, create, or forward pornographic material.
- Do not view, create, or forward chain letters or other unauthorized mass mailings.
- Do not use the "Reply-All" function to respond to e-mails with large recipient lists unless all recipients need to receive your reply.

Internet Use

What to do when you use the Internet…

- Use the Internet to support your job, activities, and responsibilities.
- You may only use the Internet for limited personal use if it does not interfere with Postal Service business or violate Postal Service policies.

What not to do when you use the Internet…

- Do not follow links to Web sites embedded in suspicious e-mail or Web advertisements.
- Do not browse pornographic, hate-based, or other sites that the Postal Service considers off-limits.
- Do not post, send, or acquire sexually oriented, hate-based, or other material the Postal Service considers off-limits.
- Do not use non-work-related applications, software, or games on Postal Service workstations or networks.
- Do not post unauthorized commercial announcements or advertising material.
- Do not promote or maintain a personal or private business.
- Do not arrange to receive news feeds and push data updates unless the material is required for Postal Service business.

Remote Access

What to do when you use remote access…

Remote Access
Access to servers from locations such as a remote office, your home, a hotel, or a non-Postal Service facility.

- If you want to use your Postal Service workstation or laptop remotely, use eAccess to ask permission from your manager.
- Use only approved computer hardware and software.
- Use only approved remote access services such as the virtual private network (VPN) or point-to-point protocol (PPP).
- Protect (via locked cabinet or closet) your Postal Service assigned devices so that unauthorized individuals cannot gain access to the device or to the Postal Service intranet.

What not to do when you use remote access…

- Do not establish a separate connection (e.g., modem or router) to the Internet while your computer is connected to the Postal Service intranet.
- Do not configure your workstation to allow unauthorized dial-in services.
- Do not connect any personal electronic devices to the Postal Service intranet or Postal Service computing devices.

Modems

What to do when you use modems…

Modems
Provide dial-up connectivity to information resources.

- If you want to install a modem, request approval from the Network Connectivity Review Board (NCRB). Complete the online NCRB Request Form located at: *https://ncrbrequest.usps.gov/NCRB.*

  Note: Approval from the NCRB is not needed for approved remote access services via VPN and PPP.
- Implement a personal firewall configured to Postal Service standards.
- Make sure that your system has been cleaned of any malicious code before connecting to the Postal Service infrastructure.
- Use approved computer hardware and software, including updated virus protection software, when sharing files with or communicating through phone lines or the Internet with the Postal Service.

- Establish approved dial-in access through Postal Service centralized dial-in services.
- Turn off modems on workstations when not in use.
- Disconnect from the Postal Service intranet before establishing alternative or additional connections to any network, such as the Internet.

What not to do when you use modems…

- Do not use a modem to connect directly to the Internet while your computer is connected to the Postal Service intranet.

Wireless Technologies

What to do when you use wireless technologies…

- If you want to use a wireless device, request approval from the NCRB by completing the online NCRB Request Form located at: *https://ncrbrequest.usps.gov/NCRB.*
- Report lost or stolen wireless devices.

What not to do when you use wireless technologies…

- Do not use Postal Service-owned equipment on home wireless networks without a personal firewall and virus protection.

4. Protection of Sensitive and Critical Information

Sensitive and Sensitive-Enhanced Information

Sensitive (hardcopy and electronic) information includes, but is not limited to, the following:

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

- Data susceptible to fraud including accounts payable, accounts receivable, payroll, and travel reimbursement.
- Information illustrating or disclosing information resource protection vulnerabilities or threats against persons, systems, operations, or facilities. Examples include information about the physical or technical aspects of a network, an DMZ, an enclave, a mainframe, a server, a workstation, including security settings, passwords, and audit logs for networks, mainframes, servers, workstations, laptop, tablets, and smart phones.

Sensitive-enhanced (hardcopy and electronic) information includes, but is not limited to, the following:

- Law enforcement information and court-restricted information, including grand jury material, arrest records, and information about ongoing investigations.
- Payment Card Industry (PCI) primary account number (PAN), i.e., full credit/debit card number (16 characters).
- Personally identifiable information (PII) including information used to distinguish or trace an individual's identity such as name, social security number, driver's 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.
- Information about individuals (e.g., employees, contractors, vendors, business partners, and customers) protected by law, including medical information and wire or money transfers.
- Information related to the protection of Postal Service restricted financial information, trade secrets, proprietary information, and emergency preparedness.
- 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).

Additional examples of sensitive and sensitive-enhanced information are included in the Business Impact Assessment (BIA) template available on:

  - The TSLC Templates Web Site under the Requirements Phase of Waterfall at: *http://itwebshare.usps.gov/sites/itweb/SitePages/TSLC%20Waterfall%20Templates.aspx.*
  - The TSLC Templates Web Site under Sprint On Phase of Agile at: *http://itwebshare.usps.gov/sites/itweb/SitePages/TSLC%20Agile%20Templates.aspx.*

When completing the BIA, an employee from the Privacy Office and the assigned Information Systems Security Officer will provide support to determine the proper information sensitivity and criticality.

How to protect sensitive information to which you have access…

- Limit hardcopy and electronic distribution to persons who have a specific job-related need for sensitive information (need-to-know).
- Limit the number of copies of sensitive information to minimum necessary.
- Cross-shred hardcopy and zero-bit format or destroy electronic copies that are not distributed or are no longer needed.
- Retain sensitive information in accordance with the retention schedule noted in the Electronic Records and Information Management System (eRIMS) at *https://erims.*
- Restrict the pickup, receipt, transfer, and delivery of sensitive information to authorized personnel.
- Protect sensitive information on Postal Service workstations, laptop computers, and hand-held devices against theft and disclosure to unauthorized individuals.
- Protect sensitive information against theft and disclosure to unauthorized individuals. This includes information stored on disks, diskettes, CDs, USB storage devices, and hardcopy.
- Encrypt sensitive information stored or archived on removable devices or media.
- Encrypt sensitive information stored off Postal Service premises.
- Encrypt sensitive information in transit across networks.
- Encrypt sensitive information in transit between an application or batch servers and a database server and between workstations and a database server.

Restricted Information The Postal Service caveat for sensitive and sensitive-enhanced information indicating access is restricted based on Postal Service regulations and policies. For more information, see the HBK AS-353, Guide to Privacy and the *Freedom of Information Act.*

- Label “RESTRICTED INFORMATION” any printed or electronic material considered sensitive, such as printouts, architecture drawings, engineering layouts, CDs, diskettes, and tapes.
- Invoke a password-protected screen saver when leaving your workstation or laptop unattended.
- Store sensitive information in a controlled area or a locked cabinet or desk.
- After receiving appropriate management approval, use factory-fresh diskettes to release electronic versions of sensitive information.
- When the retention period or legal hold has expired, destroy sensitive information in accordance with Handbook AS-805.
- Follow Postal Service disposal procedures for diskettes, CDs, and computer hardware, including disk drives and processors, containing sensitive information.
- Cross-shred hardcopy printouts and drawings containing sensitive information before disposal.
- See Handbook AS-805 for the requirements for accessing or downloading sensitive Postal Service electronic information off Postal Service premises or taking sensitive Postal Service electronic and nonelectronic information off site (i.e., non-Postal Service premises) including Postal Service data processed by business partners.
- See Handbook AS-805 for the requirements for the protection of Postal Service Information during international travel.
- Report suspicious behavior of employees, contractors, or visitors to your supervisor.

How to protect sensitive-enhanced information to which you have access…

Implement all of the protection requirements associated with sensitive information and in addition:

- Limit distribution in e-mail and hardcopy to those persons who have a specific job-related need for sensitive-enhanced information (need-to-know).
- Create an inventory listing and track sensitive-enhanced hardcopy and electronic information from creation to destruction.

If you collect credit card information:

- Protect payment card readers from the installation of skimmers.
- When accepting credit cards, ensure that the credit card information on the card is protected from view by other customers to prevent the taking of a photo of the card with a mobile phone or observation and memorization of the full credit card number.
- Ensure credit cards are signed.
- Do not accept credit cards for purchase of money orders, trust fund deposits, permit imprint deposits, purchase of pre-canceled stamps, periodical postage, postage meter setting, money-by-wire, employee debt reconciliation, COD funds, or bulk mailings.
- Follow the standard operating procedure for processing debit cards.
- Ensure that the customer has privacy when entering his personal identification number (PIN).

If you process credit card information:

- Protect credit card numbers from view by individuals that do not have a need to know.
- Do not use credit card numbers for development or testing.
- Mask credit card numbers when displayed (the first six or the last four digits are the maximum digits displayed).
- De-identify or remove credit card numbers from removable media and audit logs.
- Keep cardholder information storage to a minimum and limit retention time.
- Physically secure all hardcopy and electronic media containing cardholder data.
- Maintain strict control over internal and external distribution of cardholder data.
- Log and track all media removed from the facility.
- Encrypt PCI information throughout the life cycle.

What not to do with sensitive and sensitive-enhanced information to which you have access…

- Do not store sensitive or sensitive-enhanced information on devices not owned by the Postal Service.

- Do not co-mingle sensitive or sensitive-enhanced information with non-Postal Service information.
- Do not remove sensitive or sensitive-enhanced information from Postal Services premises without approval in writing from the functional vice president (data steward) and chief information officer or their designees.
- Do not reveal sensitive or sensitive-enhanced information without management approval.
- Do not print sensitive or sensitive-enhanced information on printers where unauthorized people may see the output.
- Do not copy sensitive or sensitive-enhanced information unless you can protect the copies.
- Do not e-mail sensitive or sensitive-enhanced information unless you are able to protect (e.g., encrypt) it.
- Do not discuss sensitive or sensitive-enhanced information in an open area where others might overhear the conversation.
- Do not send sensitive or sensitive-enhanced information by facsimile without management approval.

Critical (Moderate) Information

Critical
Essential for uninterrupted Postal Service operations or to protect health and safety of Postal Service personnel.

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

- Customer or employee life, safety, or health.
- Payment to suppliers or employees.
- Revenue collection.
- Movement of mail.
- Communications.
- Infrastructure services.
- Legal or regulatory.

Critical (High) Information

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

- Customer or employee life, safety, or health.
- Payment to suppliers or employees.
- Revenue collection.
- Movement of mail.

- Communications.
- Infrastructure services.
- Legal or regulatory requirements.

What to do with critical (moderate or high) information to which you have access…

- Protect critical information on workstations, laptop computers, and hand-held devices against theft.
- Invoke a password-protected screen saver when leaving your information resource unattended.
- Store critical information in a controlled area or a locked cabinet or desk.
- Back up critical information regularly and label copies.
- Store back-up media offsite in a secure location.

What not to do with critical (moderate or high) information to which you have access…

- Do not leave critical information in an unprotected area.

5. Protection Against Viruses and Malicious Code

Worms, Trojan Horses, and Trap Doors

Be Safe
Install the latest virus detection patterns.

Viruses and other forms of malicious code are harmful software that can contaminate, damage, or destroy information resources. Viruses can attach to e-mails, proliferate themselves, and spread automatically from computer to computer, causing widespread damage. Symptoms of infection include:

- Files or data are suddenly unavailable.
- Unexpected processes, such as e-mail transmissions or programs starting on their own.
- Files have been edited when no changes should have occurred.
- Files appear or disappear, or undergo unexpected changes in size.
- Systems display strange messages or mislabel files and directories.
- Systems become slow, unstable, or inaccessible.

Preventing Infection

What to do to prevent infection…

Watch Out
Viruses may be included in e-mail.

- Make sure your workstation and any portable computers you use for Postal Service business are equipped with virus protection software and the latest virus scanning pattern recognition file.
- Scan diskettes and removable disk drives before you use them.
- Scan incoming files before you load or save them to your computer.
- Scan files before sending them to another computer or user.
- Back up software and files frequently and maintain several generations.

What not to do . . .

- Do not download unapproved programs, shareware, or freeware from the Internet, diskette, or other media onto Postal Service equipment.
- Do not open unsolicited or suspicious e-mail or attachments.
- Do not modify the configuration of the virus protection software after installation, except as instructed by authorized personnel.
- Do not disable automatic virus scanning programs.

Responding to Infections

What to do. . .

- Stop work if you notice any symptom of infection.
- Call the Computer Incident Response Team (CIRT) at 866-USPS-CIR(T) (866-877-7247), call the Help Desk at 800-USPS-HEL(P) (800-877-7435), or send an e-mail to: *uspscirt@usps.gov.*
- Report the virus incident to your manager or supervisor.

What not to do . . .

- Do not use the computer until the CIRT or the Help Desk says it is okay to do so.
- Do not wait to report a virus incident.

6. Hardware and Software

Using and Adding Hardware and Software

What to do with hardware and software. . .

- Use only hardware and software that are approved and are included in the Infrastructure Toolkit (ITK). For information on how to add a product to the ITK:
  - Go to *http://itk.*
  - Under the heading Help is a link, ITK Request. Clicking on it will open an e-mail message. Or, you may call 202-268-4585.
- Acquire hardware and software only from official Postal Service suppliers.

What not to do with hardware and software . . .

- Do not install on Postal Service computers any unapproved software from the Internet, a diskette, CD, or other media.
- Do not use personally owned software on Postal Service computers without management approval.
- Do not violate copyright laws by using unlicensed software or making unauthorized copies of licensed software.
- Do not attach any hardware to Postal Service workstations or networks without written authorization.

7. Information Security Incidents

Recognizing Incidents

Examples of incidents that must be reported include:

- System becomes slow, unstable, or inaccessible (e.g., will not boot properly).
- Unexpected processes start without your input.
- Files disappear or undergo significant and unexpected changes in size.
- System displays strange messages or mislabels files or directories.

Information Security Incidents
Events or situations (suspected, proven, deliberate, or inadvertent) that could expose Postal Service information resources to loss or harm.

- Suspected theft of your identity.
- Stolen, missing, or damaged hardware, software, or electronic media.
- Exposed or missing hard copy files containing sensitive, sensitive-enhanced, or critical information.
- Unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information.
- Internal or external unauthorized attempts to access information resources or the facility where they reside.
- Internal or external intrusions or interference with our networks, including denial-of-service attacks, unauthorized activity on restricted systems, or unauthorized changes to files.
- Unavailability of files or data normally accessible.
- Security violations, suspicious actions, suspicion or occurrence of fraudulent activities, and potentially dangerous activities or conditions.
- Unauthorized individual in a controlled area.

Preventing Incidents

What to do to prevent information security breaches . . .

- If you do not understand any of the requirements in this handbook, ask your supervisor for clarification.
- Take the annual information security training course.
- Display proper identification when in any Postal Service facility.
- Be aware of your physical surroundings, including weaknesses in physical security and the presence of any unauthorized visitors.
- Protect Postal Service hardware, software, and sensitive, sensitive-enhanced, or critical information.

Responding to Incidents

What to do in response to a security incident. . .

- Immediately report incidents to the CIRT at 866-USPS-CIR(T) (866-877-7247) or send an e-mail to *uspscirt@usps.gov.* Employees traveling outside the United States should call 001-919-501-9299.

- Notify the following, where appropriate:
  - Help Desk at 800-USPS-HEL(P) (800-877-7435).
  - Immediate supervisor or manager.
  - Local system administrator or local technical support.
  - Security Control Officer.
  - Inspection Service local office where incident took place. If you do not know the number, you can look the number up at *https://ribbs.usps.gov/locators/find-is.cfm* or call 877-876-2455.
  - Office of Inspector General at 888-877-7644.
- Take action as directed by the CIRT.
- Document all communications and actions taken regarding the incident.
- Complete and transit to CRT PS Form 1360, *Information Security Incident Report.*

What not to do . . .

- Do not dismiss a suspected incident or discount its seriousness.
- Do not postpone reporting a suspected incident, especially a possible incident of a missing computing device in the hope that a lost device may soon be found and reporting it may be avoided; should the device subsequently be located, follow up the initial report with an immediate report indicating the device was found.

8. Monitoring of Information Resources

Why the Postal Service Monitors

The Postal Service has the legal right to monitor use of its information resources. The Postal Service monitors use to ensure these resources are protected and to verify compliance with information security policies and federal regulations. By using Postal Service information resources, you consent to the monitoring of your use of these resources. You have no expectation of privacy when using Postal Service information resources.

How You Are Notified

You are notified of monitoring through various means:

- Warning banners on electronic devices.
- Information security awareness publications, videos, and training.
- Postal Service official directives such as Handbook AS-805 and this publication, Handbook AS 805-C.

We Are Interested in Hearing From You

For more information, call Corporate Information Security at 919-501-9350 or e-mail comments to *information_security@usps.gov.*

Acknowledgement of Information Security Awareness Training

If after reading this handbook, you do not understand how to protect sensitive, sensitive-enhanced, critical (moderate), or critical (high) information, contact your manager for additional information.

Once you understand your personal responsibilities and the requirements for using established procedures to protect sensitive, sensitive-enhanced, critical (moderate), or critical (high) information:

- Send an e-mail to your manager with “Information Security Awareness Training” in the subject line or
- Make a copy of this page. Sign and date the copy and provide it to your manager.

I understand how I am personally required to protect sensitive, sensitive-enhanced, critical (moderate) or critical (high) Postal Service information to which I have access:

____
Print Name

____ __________________________
Signature Date

Blank Page

Handbook AS-805-C
PSN 7610-05-000-5604
June 2013