



INFORMATION TECHNOLOGY
Value | Knowledge | Technology

Integrity

Value

**Information
Security for
General Users**

**Handbook AS -805-C
May 2007**

Knowledge

SOLUTIONS

Confidentiality

Availability

April 2007

POSTAL SERVICE INFORMATION TECHNOLOGY USERS

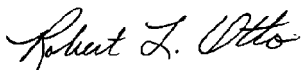
SUBJECT: Information Security Resources

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.

A handwritten signature in black ink that reads "Robert L. Otto". The signature is written in a cursive style with a large, stylized 'O' at the end.

Robert L. Otto
Vice President
Chief Technology Officer

Contents

- 1. Introduction 1**
 - What This Handbook Covers 1
- 2. Logon IDs, Passwords, PINs, and Tokens 1**
 - Getting Access 1
 - Creating a Password 2
 - Using Logon IDs and Password 2
 - Using Screensaver Time-Out and Password 3
 - Using PINs 3
 - Using Tokens 3
 - Resetting Passwords 3
- 3. Use of Information Resources 4**
 - General Use 4
 - E-mail Use 5
 - Internet Use 5
 - Remote Access 6
 - Modems 7
 - Wireless Technologies 8
- 4. Protection of Sensitive and Critical Information 8**
 - Sensitive Information 8
 - Critical Information 10
- 5. Protection Against Viruses and Malicious Code 10**
 - Worms, Trojan Horses, and Trap Doors 10
 - Preventing Infection 11
 - Responding to Infections 11
- 6. Hardware and Software 12**
 - Using and Adding Hardware and Software 12
- 7. Information Security Incidents 12**
 - Recognizing Incidents 12
 - Preventing Incidents 13
 - Responding to Incidents 13
- 8. Monitoring of Information Resources 14**
 - Why the Postal Service Monitors 14
 - How You Are Notified 14
 - We Are Interested in Hearing From You 14

1. Introduction

What This Handbook Covers

HBK AS-805

Available at
[http://blue.usps.gov/
cpim/hbkid.htm/](http://blue.usps.gov/cpim/hbkid.htm/)

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

Baseline Information Services

Active Directory
Account, e-mail, and
office suite.

eAccess

Online computer
request
application at
[https://eaccess.
usps.gov](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.

Don't have access now?

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.

- 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 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.

What not to do when using logon IDs and passwords...

Screensaver
Protects information when user is away from computer but not logged out.

- Never let anyone use your logon ID or password and don't use anyone else's.
- Do not write down your password or reveal it to anyone.
- Do not store your password in application code, files, or tables.

Using Screensaver Time-Out and Password

- Make sure your screensaver time-out feature is working.

Using PINs

PIN
Used primarily for selected applications.

- Protect PINs as you protect passwords.

Using Tokens

Token
Hardware device you 'have' that can be used for authentication.

- Protect tokens from theft and do not allow others to use them.

Resetting Passwords

- If you suspect your password has been compromised, change it 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>)
 - Mainframe Password (<https://hcssupport.usps.gov/reset>)

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-660-2004-3, *Limited Personal Use of Government Office Equipment Including 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.
- 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.usps.gov/itk_new/. Click on Access ITK on the right-hand side. You will get a list of approved software.

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 private files or accounts.
- Do not perform unofficial activities that could degrade the performance of our equipment or systems, such as play electronic games.
- Do not use Postal Service resources to promote or maintain a personal or private business or commit fraudulent or illegal activities.
- Do not bring personal electronic devices (e.g., laptops, notebooks, personal digital assistants [PDAs], handheld computers, or storage media including universal serial bus [USB] thumb drives) into Postal Service facilities.
- 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.

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) or violate policies.
- Send sensitive information and non-publicly available information only to authorized personnel who "need-to-know."
- Use Postal Service-approved encryption software to encrypt sensitive information (e.g., personally identifiable information [PII] and credit and debit cardholder information) sent by e-mail and give management recovery keys and decryption instructions.

What not to do when you use email . . .

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

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

- Never use Postal Service computers to check your personal e-mail accounts, such as Hotmail, Yahoo, MSN, AOL, or other e-mail service providers.
- Do not open suspicious e-mail attachments.
- Do not send information that violates state or federal laws; 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.
- Do not send or respond to spam. Delete it.
- Do not create or forward pornographic material.
- Do not create or forward chain letters or other unauthorized mass mailings.

Internet Use

What to do when you use the Internet. . .

- Use the Internet primarily to support your job.
- You may use the Internet for limited personal use *only* if it doesn't interfere with Postal Service business or violate our policies.

What not to do when you use the Internet . . .

- 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

Used to access 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 remote workstation or laptop 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 internal network.
- Do not configure your workstation to allow unauthorized dial-in services.
- Do not connect personal electronic devices to the Postal Service Intranet.

Modems

What to do when you use modems. . .

Modems

Used to provide dial-up connectivity to information resources.

NCRB

<http://it.usps.gov>

- If you want to install a modem, request approval from the Network Connectivity Review Board (NCRB). To get a request form:
 - Go to the NCRB Web site (<http://it.usps.gov>).
 - Click on Support at the top of the page. In the drop-down box, select Corporate Information Security, then Network Connectivity Review Board (NCRB).
 - Scroll down to Request Form and open the link to the request form.

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 Network Connectivity Review Board (NCRB). To get a form, follow the directions under “Modem, What to do...”, on the previous page.
- 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

Restricted access within or disclosure outside of Postal Service consistent with Privacy Act, FOIA, and Postal Service policy. See HBK AS-805, chapter 3.

Restricted Information

Restricted access based on Postal Service regulations and policies. For more information see the HBK AS-353, *Guide to Privacy and the Freedom of Information Act*.

In this section, sensitive information includes business-controlled sensitive information and critical information includes business-controlled critical information.

Sensitive Information

What to do about sensitive information . . .

- Know what information is sensitive. When in doubt, consult the official criteria for the determination of sensitive information, which can be found on the Privacy Office Web site, <http://blue.usps.gov/caweb/privacy/>.
- Restrict access to sensitive information to authorized personnel who “need to know.”
- 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 about the Postal Service against theft and disclosure to unauthorized individuals. This includes information stored on disks, diskettes, CDs, and USB storage devices.

- Encrypt sensitive information (e.g., PII and cardholder information) stored or archived on removable devices or media.
- Encrypt sensitive information (e.g., PII and cardholder information) stored off Postal Service premises.
- Encrypt sensitive information (e.g., PII and cardholder information) in transit across networks.
- Label “RESTRICTED INFORMATION” any printed or electronic material considered sensitive, such as printouts, architecture drawings, engineering layouts, disks, diskettes, and tapes.
- Invoke a password-protected screen saver when leaving your information resource 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.
- Inventory and track sensitive information from creation to destruction.
- Follow Postal Service disposal procedures for diskettes, CDs, and computer hardware, including disk drives and processors, containing sensitive information.
- Shred hardcopy printouts and drawings containing sensitive information before disposal.

What not to do with sensitive information . . .

- Do not store Postal Service information on devices not owned by the Postal Service.
- Do not commingle Postal Service information not available to the public with non-Postal Service information.
- Do not remove sensitive information from Postal Services premises without approval in writing from the functional vice president (data steward) and chief information officer (CIO) or their designees.
- Do not reveal sensitive information without management approval.
- Do not print sensitive information on printers where unauthorized people may see the output.
- Do not copy sensitive information unless you can protect the copies.

- Do not e-mail sensitive information unless you are able to protect (e.g., encrypt) it.
- Do not discuss sensitive information in an open area where others might overhear the conversation.
- Do not send sensitive information by facsimile without management approval.

Critical Information

What to do with critical information. . .

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

- Protect Postal Service workstations, laptop computers, and hand-held devices.
- Use password-protected, time-out feature on screensavers.
- Back up information regularly and label copies.
- Store back-up media offsite in a secure location.

What not to do with critical information . . .

- Do not leave critical information in an unprotected area.

5. Protection Against Viruses and Malicious Code

Worms, Trojan Horses, and Trap Doors

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:

Be Safe
Install the latest virus detection patterns.

- 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 often
hitchhike on 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 from an unknown source before sending them to another computer.
- 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 fail 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 appear 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 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 copying software without authorization.
- Do not attach any hardware to Postal Service workstations or networks without authorization.

7. Information Security Incidents

Recognizing Incidents

Examples of incidents that must be reported include:

- Missing or damaged hardware, software, or electronic media.

Information Security Incidents

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

- 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 . . .

- 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 visitor.

Responding to Incidents

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

- Immediately report incidents to the Computer Incident Response Team (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 (SCO).
 - Inspection Service local office where incident took place. If you do not know the number, you can look the number up at <http://www.usps.com/ncsc/locators/findis.html> or call 877-876-2455.

- Office of Inspector General (OIG) at 888-877-7644.
- Take action as directed by the CIRT.
- Document all communications and actions taken regarding the incident.
- Complete PS Form 1360, *Information Security Incident Report*.

What not to do . . .

- Do not dismiss a suspected incident or discount its seriousness.

8. Monitoring of Information Resources

Why the Postal Service Monitors

The Postal Service has the legal right to monitor use of its information resources. It monitors use to make sure that these resources are protected and that information security policies and federal regulations are honored. By using Postal Service information resources, you consent to monitoring.

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 HBK AS-805 and this document you are now reading.

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.