

November 2002

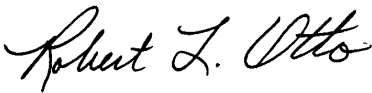
To users of Postal Service information resources:

If you are a Postal Service employee, contractor, vendor, or business partner who uses our information resources, this handbook is for you. It summarizes what you need to know about using these 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.

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

Robert L. Otto  
Vice President  
Information Technology

# Contents

<b>1. Introduction</b>	<b>1</b>
What This Book Covers	1
<b>2. Logon IDs, Passwords, and PINS</b>	<b>1</b>
Getting Access	1
Creating A Password	2
Using logon IDs and Passwords	2
Using Screensaver Time-Out and Password	3
Using PINs	3
<b>3. Use of Information Resources</b>	<b>3</b>
General Use	3
E-mail Use	4
Internet Use	4
Remote Access	5
Modems	5
<b>4. Protection of Sensitive and Critical Information</b>	<b>6</b>
Sensitive Information	6
Critical Information	7
<b>5. Protection Against Viruses and Malicious Code</b>	<b>7</b>
Worms, trojan horses, trap doors, “oh my!”	7
Preventing Infection	8
Responding to Infections	9

<b>6. Hardware and Software</b> .....	<b>9</b>
Using and Adding Hardware and software .....	9
<b>7. Information Security Incidents</b> .....	<b>10</b>
Recognizing Incidents .....	10
Preventing Incidents .....	10
Responding to Incidents .....	11
<b>8. Monitoring of Information Resources</b> .....	<b>12</b>
Why the Postal Service Monitors .....	12
How You Are Notified .....	12

# 1. Introduction

## HBK AS-805

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

## What This Book Covers

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

# 2. Logon IDs, Passwords, and PINS

## Basic Computer Services

Local Area Network, e-mail, Internet, and office suite.

## Getting Access

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

## eAccess

Online computer request application at  
<http://eaccess.usps.gov>.

## Logon ID

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

### Don't have access now?

If you don't have access but need it to do your job, your supervisor or manager will request it via eAccess, and you will receive a logon ID via e-mail from Information Technology when access is approved.

### 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 via eAccess.

## Creating A Password

### Password

A string of characters used with a logon ID to identify a user.

#### What to do . . .

- Use at least six-character alphanumeric passwords.
- Choose one that is hard for others to guess, like phrases or word strings.
- Use characters from at least three of the following:
  - Uppercase letters.
  - Lowercase letters.
  - Numbers (0–9).
  - Special characters (like &, #, and \$).
- See HBK AS-805 if you are a privileged user or work in technology.

#### What not to do . . .

- Do not use your name, family members' names, birthdate, or other personal information.
- Do not use terms like *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.

## Using logon IDs and Passwords

#### What to do . . .

- Keep your password confidential. You are accountable for actions performed by anyone using your logon ID and password, even if you didn't give them permission.
- Change your password if you think it has been compromised.

#### What not to do . . .

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

**Screensaver**

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

## Using Screensaver Time-Out and Password

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

**PINS**

Used primarily for selected applications.

## Using PINs

- Protect PINs like you protect passwords.

# 3. Use of Information Resources

## General Use

### What to do . . .

#### Limited Personal Use

See HBK AS-805, ch.5, and MI EL-660-2000-5.

- 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.

### What not to do . . .

- 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 another's private files or accounts.
- Do not perform unofficial activities that could degrade the performance of our information resources, such as playing electronic games.
- Do not use our resources to promote or maintain a personal or private business or commit fraudulent or illegal activities.

### **Restricted Information**

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

### **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.

## **E-mail Use**

### **What to do . . .**

- You may use Postal Service e-mail for occasional personal use *only* if it doesn't interfere with Postal Service business or violate policies.
- You may encrypt restricted information you send by e-mail if you use Postal Service-approved encryption software and provide management with keys and instructions.

### **What not to do . . .**

- Never use Postal Service computers to check your personal e-mail accounts, such as Hot Mail, Yahoo, MSN, AOL, etc.
- Do not open suspicious e-mail attachments.
- Do not send information that violates state or federal laws or 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.
- 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 . . .**

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

### What not to do . . .

- Do not browse pornographic, hate-based, or other sites that the Postal Service considers off-limits.
- Do not post, send, or acquire sexually oriented material, 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 . . .

- Request approval to use it from your manager via eAccess.
- 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 your remote workstation or laptop so that unauthorized personnel do not use it to access the Postal Service internal network.

### What not to do . . .

- 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.

#### Remote Access

Used to access information resources from locations such as a remote office, your home, a hotel, or a non-Postal Service facility.

# Modems

## What to do . . .

### **Modems**

Used to provide dial-up connectivity to information resources.

### **NCRB**

<http://ncrb.usps.gov>

- Request approval from the Network Connectivity Review Board (NCRB). Use the form on the NCRB web site under *Request Forms*. (Approval 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 internal network prior to establishing alternative or additional connections to any network, such as the Internet.

## What not to do . . .

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

# 4. Protection of Sensitive and Critical Information

## Sensitive Information

### **Sensitive**

Restricted access within or disclosure outside of Postal Service consistent with Privacy Act, FOIA, and Postal Service policy. See HBK AS-805, ch. 4.

### **Restricted Information**

Restricted access based on Postal Service regulations and policies. See ASM, ch. 3.

#### What to do . . .

- Know what information is sensitive. When in doubt, ask your supervisor or manager.
- Restrict access to it to authorized personnel.
- Protect it on Postal Service workstations, laptop computers, and hand-held devices.
- Encrypt transmissions over any untrusted network, such as the Internet.
- Label hardcopy and screens as “Restricted Information.”
- Lock up or shred all hard-copy printouts.
- Use factory-fresh diskettes to release electronic versions of information.
- Follow Postal Service retirement and disposal procedures for old diskettes or computer hardware, including disk drives and processors.

#### What not to do . . .

- Do not reveal sensitive information without management approval.
- Do not print it on printers where unauthorized people may see the output.
- Do not copy it unless you protect the copies appropriately.
- Do not e-mail it unless you are able to protect it.
- Do not discuss it in an open area where others might overhear the conversation.
- Do not FAX it without management approval.

## Critical Information

### What to do . . .

**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 on a regular basis and label copies.
- Store back up media offsite in a secure location.

### What not to do . . .

- Do not locate critical information in an unprotected area.

## 5. Protection Against Viruses and Malicious Code

### Worms, trojan horses, trap doors, *“oh my!”*

**Watch Out**  
Viruses often  
hitchhike on e-mail.

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, self-start.
- Files have been edited, though 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 . . .

**Be Safe**  
Install the latest  
virus detection  
patterns.

- Make sure your workstation and any portable and home 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 untrusted 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 information resources.
- 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 1-866-USPS-CIR(T) (1-866-877-7247) or
- Call the Help Desk at 1-800-USPS-HEL(P) (1-800-877-7435).
- 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 OK.
- Do not fail to report a virus incident.

## 6. Hardware and Software

### Using and Adding Hardware and software

#### What to do . . .

- Use only hardware and software that appear in the *Infrastructure Toolkit* (ITK). To add a product to the ITK, go to <http://itk>, click on *ITK Change Request Forms*, click on *Addition of a New Product Form*, and follow the directions.
- Acquire hardware and software from official Postal Service suppliers.

### What not to do . . .

- Do not install on Postal Service computers unapproved software obtained 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

#### **Information Security Incidents**

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

Examples of incidents that must be reported include:

- Loss, theft, or destruction of information resources, such as missing or damaged hardware, software, or electronic media.
- 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 . . .

- 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 . . .

- Immediately report incidents to the Computer Incident Response Team (CIRT) at 1-866-USPS-CIR(T) (1-866-877-7247) or send an e-mail to [uspscirt@email.usps.gov](mailto:uspscirt@email.usps.gov).
- Notify the following, where appropriate:
  - Help Desk at 1-800-USPS-HEL(P) (1-800-877-7435).
  - Immediate supervisor or manager.
  - Local system administrator or local technical support.
  - Corporate Information Security at 1-919-501-9350.
  - Security Control Officer (SCO).
  - Inspection Service.
  - Office of Inspector General (OIG) at 1-888-877-7644
- Take action as directed by the CIRT.
- Document all conversations and actions taken regarding the incident.
- Complete 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 information resources.
- Information security awareness publications, videos, and training.
- Postal Service official directives, like HBK AS-805 and this document you are now reading.

**NOTES**

**We are interested in hearing from you.**

For more information, call Corporate Information Security at 1-919-501-9229 or e-mail comments to [iscomm@email.usps.com](mailto:iscomm@email.usps.com). You can also mail comments to:

CORPORATE INFORMATION SECURITY  
UNITED STATES POSTAL SERVICE  
4200 WAKE FOREST ROAD  
RALEIGH NC 27668-1510

Additional copies of this handbook are available from the material distribution center. You can also access this guide online at <http://blue/cpim/hbkid.htm>.