Contents

This page intentionally left blank

1 Introduction: Corporate Information Security

1-1 Purpose

The Postal Service is committed to creating and maintaining an environment that protects Postal Service information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. Handbook AS-805, *Information Security,* establishes the information security policies to appropriately identify, classify, and protect those information resources. Adherence to information security policies will safeguard the integrity, confidentiality, and availability of Postal Service information and will protect the interests of the Postal Service, its personnel, its business partners, and the general public.

Information security policy will ensure the creation and implementation of an environment that:

a. Protects information resources critical to the Postal Service.

b. Protects information as mandated by federal laws, regulations, directives, law enforcement and judicial processes, and industry requirements.

c. Protects the personal information and privacy of employees and customers.

d. Reinforces the reputation of the Postal Service as an institution deserving of public trust.

e. Complies with due diligence standards for the protection of information resources.

f. Assigns responsibilities to relevant Postal Service officers, executives, managers, employees, contractors, partners, and vendors.

The following principles guide the development and implementation of Postal Service information security policies and practices:

a. Information is:

- A critical asset that must be protected.
- Restricted to authorized personnel for authorized use.

b. Information security is:

- Cornerstone of maintaining public trust.
- A business issue — not a technology issue.
- Risk based and cost effective.

- Aligned with Postal Service priorities, industry-prudent practices, and government requirements.
- Directed by policy but implemented by business owners.
- Everybody's business.

1-2 Scope

Information security applies to all information resources, organizations, and personnel. Chapter 1 addresses the following:

a. Information resources.

b. Organizations and personnel.

c. Importance of Compliance.

1-3 Policy

The Postal Service information security policies are grouped in the following areas:

a. Security roles and responsibilities.

b. Information designation and control.

c. Security risk management.

d. Acceptable use.

e. Personnel security.

f. Physical and environmental security.

g. Development and operations security.

h. Information security services.

i. Hardware and software security.

j. Corporate network security.

k. Business continuity management.

l. Security incident management.

m. Security compliance and monitoring.

Information resources that collect information about individuals are subject to the Privacy Act.

The Privacy Act requires all federal agencies, including the Postal Service, to adhere to a minimum set of standards for the collection and processing of personal data and restricts the disclosure of such Privacy Act information. Agencies are required to establish appropriate administrative, technical, and physical safeguards to protect Privacy Act data. These safeguards ensure the security and confidentiality of information resources containing Privacy Act data and protect against unauthorized disclosure of such data, which could result in substantial harm, embarrassment, unfairness, or inconvenience to an individual.

1-4 Supporting Documentation

The following handbooks provide implementation guidelines for this handbook:

a. Handbook AS-805-A, *Information Resource Certification and Accreditation Process.*

b. Handbook AS-805-D, *Information Security Network Connectivity Process.*

c. Handbook AS-805-G*, Information Security for Mail Processing Equipment/Mail Handling Equipment* (MPE/MHE).

1-5 Policy Owner

The policy owner of this handbook is the manager of the Corporate Information Security Office.

1-6 Information Resources

Information security policies apply to all information, in any form, related to Postal Service business activities, employees, or customers that have been created, acquired, or disseminated using Postal Service resources, brand, or funding. Information security policies apply to all technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information. Information security policies also apply to all information systems, infrastructure, applications, products, services, telecommunications networks, computer-controlled mail processing equipment, and related resources, which are sponsored by, operated on behalf of, or developed for the benefit of the Postal Service.

Information technologies and the information they contain are collectively known as information resources (see Exhibit 1-6 for examples). Information resources may be referred to as technology solutions within the Technical Solutions Life Cycle (TSLC).

Exhibit 1-6
Examles of Information Resources

Category	Description	Examples
Systems and Equipment	All multi-user computers and computer-controlled systems and their components.	■ Data Processing ■ Automated Information Systems (AIS) ■ Process Control Computers ■ Process Control Systems ■ Embedded Computer Systems ■ Mainframe Computers ■ Minicomputers ■ Microcomputers ■ Microprocessors ■ Office Automation Systems ■ Stand-Alone, Shared Logic, or Shared Resource Systems ■ Firmware ■ Servers ■ Kiosks ■ Intelligent Vending Machines
Mail Processing Equipment	All computer-controlled equipment and networks used in processing, distributing, and transporting the mail.	■ Bar Code Sorters ■ Flat Sorters ■ Optical Character Readers ■ Data Collection System ■ Routers and Switches ■ Tray Management System ■ Forwarding Control System ■ National Directory Support System
Single-User Computer Equipment	All computers and their components used by individuals.	■ Personal Computers (PCs) ■ Workstations ■ Laptop Computers ■ Notebook Computers ■ Personal Digital Assistants (PDAs) ■ Palm Tops ■ Handheld Computers
Hardware	All major items of equipment or their components associated with a computer system.	■ Central Processing Units (CPUs) ■ Terminals ■ Monitors ■ Speakers ■ Video Display Terminals ■ Projection Equipment ■ Modems ■ Printers
Software	All programs, scripts, applications, operating systems, HTML, and related resources.	■ Operating Systems (OS) ■ Programs ■ Applications ■ Applets ■ Database Management Systems ■ Custom Code ■ Associated Documentation

Category	Description	Examples
Data and Information	All information or data stored in digital format, or as a printed product of data stored in digital format.	■ Text Files ■ Documents ■ Spreadsheets ■ Digital Images ■ Electronic Mail ■ Tables ■ Databases ■ Biometrics Information
Products and Services	All objects, processes, functions, and information delivered by, for, or under the brand of the Postal Service.	■ Information Delivery Services ■ E-Commerce Applications ■ Digital Certificate Services ■ Web Site Content
Network Facilities	All communications lines and associated interconnected communications equipment.	■ Transition Lines ■ Terminal Equipment ■ Routers ■ Firewalls ■ Hubs ■ Switches ■ Local Area Networks (LANs) ■ Wide Area Networks (WANs) ■ Virtual Private Networks (VPNs) ■ Infrastructure ■ Internet ■ Intranet ■ Extranet ■ Telephone and Telephone Systems ■ Voice-Messaging Systems ■ Fax Machines ■ Videoconferencing Equipment ■ Wireless Communications
Media	All electronic and nonelectronic media used for information exchange.	■ Magnetic Tapes ■ Magnetic or Optical Disks ■ Diskettes ■ USB Devices ■ Hard-Copy Printouts

1-7 Organizations and Personnel

Information security policies apply to all Postal Service functional organizations and personnel, including Postal Service employees, contractors, vendors, business partners, and any other authorized users of Postal Service information systems, applications, telecommunication networks, data, and related resources. Information security applies to the Office of the Inspector General and the Inspection Service except where statutory authority exempts them.

For the purposes of these policies, the above entities are collectively known as personnel. This definition of “personnel” excludes customers whose only

access is through publicly available services, such as public Web sites of the Postal Service.

These policies do not change the rights or responsibilities of either management or the unions pursuant to Articles 17 and 31 of the various collective bargaining agreements or the National Labor Relations Act, as amended. These revisions do not bar the unions from using their own portable devices and media for processing information that is relevant for collective bargaining and/or grievance processing, including information provided by management pursuant to Articles 17 and 31 of the collective bargaining agreement or the National Labor Relations Act. There is no change to policy concerning restricted access to the Postal Service Intranet.

Note: For specific guidance regarding practices or actions not explicitly covered by these policies, contact the manager, Corporate Information Security Office, prior to engaging in such activities.

1-8 Importance of Compliance

1-8.1 Maintaining Public Trust

The public entrusts vast amounts of information to the Postal Service every day — information that the Postal Service is required by law and good business practice to protect. Compliance with information security policies will help protect information resources and enhance the reputation of the Postal Service as deserving of public trust.

1-8.2 Continuing Business Operations

The Postal Service is committed to delivering superior customer service in an increasingly competitive marketplace through the effective use of technology, information, and automation. Compliance with information security policies will help ensure the continuous availability and integrity of the technological infrastructure that is critical to the Postal Service's ability to perform its mission.

1-8.3 Protecting Postal Service Investment

Postal Service information resources represent a sizable financial investment in technologies and in information that can never be replicated. These information resources are of paramount importance to the mission of the Postal Service and to the country and must be protected.

1-8.4 Abiding by Federal Regulations

Postal Service information security policies are designed to respond to the intent and spirit of government regulations and directives.

1-8.5 Granting an Exception to the Policies

Any exception to the policies in this handbook must be based on risk acceptance and approved by the Chief Information Officer and Executive Vice President. If the exception impacts sensitive or sensitive-enhanced information, the Chief Privacy Officer must also approve. (Information categories and levels are defined in 3-2, Information Designation and Levels, of this handbook).

This page intentionally left blank

2 Security Roles and Responsibilities

2-1 Policy

Information security is the individual and collective responsibility of all Postal Service personnel, business partners, and other authorized users. Access to information resources is based on an individual's roles and responsibilities. Only authorized personnel are approved for access to Postal Service information resources.

All information technology managers are responsible for securing the Postal Service computing environment, which includes information resources and infrastructure, by implementing appropriate technical and operational security processes and practices that comply with Postal Service information security policies.

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for implementing information security policies. All officers and managers must ensure compliance with information security policies by organizations and information resources under their direction and provide the personnel, financial, and physical resources required to appropriately protect information resources.

All Postal Service personnel, including employees, consultants, subcontractors, business partners, and customers who access nonpublicly available Postal Service information resources (e.g., mainframes and the Postal Service intranet) and other authorized users of Postal Service information resources are responsible for complying with all Postal Service information security policies.

2-2 Consolidated Roles and Responsibilities

2-2.1 Chief Information Officer

The chief information officer (CIO) is responsible for the following:

a. Acting as the senior information technology (IT) decision maker and corporate change agent to securely integrate the key components of business transformation: technology, processes, and people.

b. Providing advice and assistance to senior managers on information security policy and their compliance-based performance.

c. Promoting the implementation of an information security architecture to mitigate information security-related risk.

d. Promoting the protection of corporate information resources across Postal Service organizations and business partners.

2-2.2 Chief Postal Inspector

The chief postal inspector is responsible for the following:

a. Establishing policies, procedures, standards, and requirements for personnel, physical, and environmental security.

b. Approving the identification of sensitive positions.

c. Conducting background investigations and granting personnel clearances.

d. Conducting site security reviews, surveys, and investigations of facilities containing Postal Service computer and telecommunications equipment to evaluate all aspects of physical, environmental, and personnel security.

e. Providing technical guidance on physical and environmental security activities that support information security, such as controlled areas, access lists, physical access control systems, and identification badges; providing protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

f. Providing security consultation and guidance during system, application, and product development to assure that security concerns are addressed and information and/or evidence that may be needed for an investigation is retained by the information resource.

g. Assisting the manager, Corporate Information Security Office (CISO), with reviews, as appropriate.

h. Investigating reported security violations and conducting revenue/financial investigations including theft, embezzlement, or fraudulent activity.

i. Providing physical protection and containment assistance and investigating information security incidents as appropriate.

j. Funding CISO investigative efforts outside of those normally required.

k. Managing, securing, scanning, and monitoring the Inspection Service's network and information technology infrastructure.

2-2.3 Vice President, Information Technology Operations

The vice president, Information Technology Operations (VP IT Operations), is responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of data.

c. Ensuring the protection and secure implementation of the Postal Service IT infrastructure.

d. Ensuring compliance with the information security assurance processes.

e. Together with the vice president of the functional business area, accepting, in writing, residual risk of applications and approving deployment. The VP IT Operations may delegate this responsibility to the applicable portfolio manager.

f. Together with the vice president of the functional business area, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. (If this responsibility is delegated, notice to that effect must be writing.)

g. Reporting to senior management on the status of an incident at a major IT site.

2-2.4 Manager, Corporate Information Security Office

The manager, CISO, is responsible for the following:

a. Setting the overall strategic and operational direction of the Postal Service information security program and the program's implementation strategies.

b. Engaging at any point on any level for issues related to information security that impact the Postal Service.

c. Recommending members to the Information Security Executive Council.

d. Developing information security policies, processes, standards, and procedures.

e. Managing the certification and accreditation (C&A) process.

f. Providing guidance on application security, reviewing the C&A documentation package, and accrediting sensitive-enhanced, sensitive, and critical information resources developed for, endorsed by, or operated on behalf of the Postal Service.

g. Managing the Network Connectivity Review Board (NCRB) process.

h. Authorizing temporary access to information resource services.

i. Conducting site security reviews or providing support to the Postal Inspection Service during its site security reviews, as requested.

j. Providing consulting support for securing the network perimeter, infrastructure, integrity controls, asset inventory, identification, authentication, authorization, intrusion detection, penetration testing, and audit logs and for information security architecture, technologies, procedures, and controls.

k. Approving encryption technologies.

l. Providing leadership of the Security Forum for the Enterprise Architecture Forum.

m. Developing and implementing a comprehensive information security training and awareness program.

n. Serving as the central point of contact for all information security issues and providing overall consultation and advice on information security policies, processes, standards, procedures, requirements, controls, services, and issues.

o. At least annually, assessing the adequacy of information security policy and process to reflect changes to business objectives and the operating environment (including technology infrastructure, threats, vulnerabilities, and risks) and assessing the adequacy of information security controls and recommending changes as necessary.

p. Establishing evaluation criteria and recommending security hardware, software, and audit tools.

q. Approving the establishment of shared accounts.

r. Ensuring compliance to information security policies and standards through inspections, reviews, and evaluations.

s. Providing support to the Office of the Inspector General (OIG) and the Inspection Service during the conduct of investigative activities concerning information security, the computing infrastructure, and network intrusions, as requested.

t. Providing support to the chief postal inspector during the conduct of facility/site security reviews, as requested.

u. Escalating security issues to executive management and promulgating security issues and recommended corrective actions across the Postal Service.

v. Authorizing monitoring and surveillance activities of information resources.

w. Authorizing (in case of threats to the Postal Service infrastructure, network, or operations) appropriate actions that may include viewing and/or disclosing data to protect Postal Service resources or the nation's communications infrastructure.

x. Confiscating and removing any information resource suspected of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be used in forensic analysis of a security incident.

y. Reviewing and approving information security policy for mail processing equipment/mail-handling equipment (MPE/MHE).

2-2.5 Information Security Executive Council

The Information Security Executive Council consists of appropriate Postal Service representatives and serves as a steering committee advising the CISO and promulgating information security throughout the Postal Service.

2-2.6 Vice Presidents, Functional Business Areas

The vice presidents of Postal Service functional business areas are responsible for the following:

a. Ensuring resources are available for completing information security tasks.

b. Ensuring the security of all information resources within their organization.

c. Together with the VP IT Operations, accepting, in writing, residual risks associated with information resources under their control and approving deployment. The vice presidents of functional business areas have delegated this responsibility to the applicable executive sponsor.

d. Ensuring that contractual agreements require all contractors, vendors, and business partners to adhere to Postal Service information security policies.

e. Together with the VP IT Operations, approving the removal of portable electronic devices or media containing sensitive-enhanced or sensitive information from a Postal Service facility. (If this responsibility is delegated, the delegation of responsibility must be writing.)

2-2.7 Vice President, Engineering

The vice president, Engineering, is responsible for ensuring the security of information resources used in support of the MPE/MHE environment, including technology acquisition, development, and maintenance.

2-2.8 Vice President, Network Operations Management

The vice president, Network Operation Management, is responsible for the security of the mail and information resources used in support of MPE/MHE strategies and logistics.

2-2.9 Officers and Managers

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for the following:

a. Implementing information security policies, ensuring compliance with information security policies by organizations and information resources under their direction, and invoking user sanctions as required.

b. Identifying sensitive information positions in their organizations and ensuring that personnel occupying sensitive positions hold the appropriate level of clearance.

c. Managing access authorizations, documenting information security responsibilities for all personnel under their supervision, and ensuring they receive information security training commensurate with their responsibilities and comply with Postal Service information security policies and procedures.

d. Including employee information security performance in performance evaluations.

e. Supervising information security responsibilities of their contractor personnel.

f. Processing departing personnel appropriately and notifying the appropriate system and database administrators when personnel no longer require access to information resources.

g. Initiating a written request for message and data content monitoring and sending it to the chief privacy officer (CPO) for approval.

h. Approving or denying requests, by personnel under their supervision, for access to information resources beyond temporary information resource services and reviewing those access authorizations on a semiannual basis.

i. Ensuring that all hardware and software are obtained in accordance with official Postal Service processes.

j. Protecting information resources and ensuring their availability through business continuity activities including plans, procedures, off-site backups, periodic testing, workarounds, and training/cross-training essential and alternate personnel.

k. Ensuring that personnel under their supervision who remove a portable electronic device or media from a Postal Service facility are aware of their responsibility for its security and have a place to secure the device or media when it is not being used.

l. Ensuring compliance with Postal Service information security policy and procedures.

m. Reporting suspected information security incidents to the Computer Incident Response Team (CIRT) in a timely manner, protecting information resources at risk during security incidents, containing the incident, and following continuity plans for disruptive incidents (see Chapter 13, Security Incident Management).

2-2.10 Executive Sponsors

Executive sponsors, as representatives of the vice president of the functional business area, are the business managers with oversight (e.g., funding, development, production, and maintenance) of the information resource and are responsible for the following:

a. Consulting with the CPO for determining information sensitivity and Privacy Act applicability.

b. Conducting a business impact assessment (BIA) to determine the sensitivity and criticality of each information resource under his or her control and to determine the potential consequences of information resource unavailability.

c. Providing resources to ensure that security requirements are properly addressed and information resources are properly protected.

d. Ensuring completion of a site security review, if the facility hosts an information resource designated as sensitive-enhanced, sensitive, or critical.

e. Ensuring that contract personnel under their supervision comply with Postal Service information security policies and procedures.

f. Ensuring that all information security requirements are included in contracts and strategic alliances.

g. Ensuring compliance with, and implementation of, the Postal Service privacy policy, data collection policy, customer privacy statement, and software licensing.

h. Appointing, in writing, an information systems security representative (ISSR).

i. Ensuring completion of security-related activities throughout the Information resource C&A life cycle.

j. Ensuring that information resources within their purview are capable of enforcing appropriate levels of information security services to ensure data integrity.

k. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.

l. Authorizing access to the information resources under their control and reviewing those access authorizations on a semiannual basis.

m. Maintaining an accurate inventory of Postal Service information resources and coordinating hardware and software upgrades.

n. Ensuring appropriate funding for proposed business partner connectivity, including costs associated with the continued support for the life of the connection.

o. Initiating and complying with the network connectivity request requirements and process as documented in the Information Security Network Connectivity Process.

p. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

q. Funding application recovery (including but not limited to hardware/ software licenses required, continuity plan development, testing, and maintenance) for applications.

r. Working jointly with the portfolio manager to review the C&A documentation package, accept the residual risk to an application, and approve the application for production or return the application to the applicable life cycle phase for rework.

s. Reporting suspected information security incidents to the CIRT in a timely manner, protecting information resources at risk during the security incident, containing the incident, and following continuity plans for disruptive incidents.

2-2.11 Portfolio Managers

Portfolio managers are responsible for the following:

a. Supporting the executive sponsor in the development of information resources and the C&A process, including the BIA, risk assessment, and business continuity plans.

b. If an ISSR has not been assigned by the executive sponsor, appointing an ISSR to perform security-related activities.

c. Providing coordination and support to executive sponsors and disaster recovery (DR) service providers for all matters relating to business continuity planning.

d. Reviewing the C&A documentation package and completing a risk-mitigation plan for risks identified as high or medium. If a documented vulnerability will not be mitigated, preparing and signing an acceptance of responsibility letter as part of the C&A process.

e. Working jointly with the executive sponsor to review the C&A documentation package, accept the residual risk to an information resource, and approve the information resource for production or return the information resource to the applicable life cycle phase for rework.

f. Ensuring that the information resource is registered in eAccess.

g. Accepting personal accountability for adverse consequences if the information resource was placed in production before the C&A process was completed.

h. Managing projects through their project managers who are responsible for the following:

(1) Incorporating the appropriate security controls in all information resources.

(2) Developing C&A documentation as required.

(3) Ensuring that the information resource is entered in the Enterprise Information Repository (EIR) and updated as required.

2-2.12 Managers of Major Information Technology Sites

Managers of major IT sites are responsible for the following:

a. Functioning as the incident management team leader for their facility.

b. Identifying and training key technical personnel to provide support in business continuity planning for their facility, information resources housed in their facility, and the alternate DR facilities.

2-2.13 Installation Heads

Installation heads are in charge of Postal Service facilities or organizations, such as areas, districts, Post Offices, mail processing facilities, parts depots, vehicle maintenance facilities, computer service centers, or other installations. Installation heads are responsible for the following:

a. Designating a security control officer (SCO) who is responsible for personnel and physical security at that facility, including the physical protection of computer systems, equipment, and information located therein.

b. Implementing physical and environmental security support for information security, such as the protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

c. Controlling physical access to the facility, including the establishment and implementation of controlled areas, access lists, physical access control systems, and identification badges.

d. Funding building security equipment and security-related building modifications.

e. Maintaining an accurate inventory of Postal Service information resources at their facilities and implementing appropriate hardware security and configuration management.

f. Maintaining and upgrading all security investigative equipment, as necessary.

g. Ensuring completion of a site security review, providing assistance to the Inspection Service and CISO as required, and accepting site residual risk.

h. Ensuring that the Postal Service security policy, standards, and procedures are followed in all activities related to information resources (including procurement, development, and operation) at their facility.

i. Ensuring that all employees who use or are associated with the information resources in the facility are provided information security training commensurate with their responsibilities and taking appropriate action in response to employees who violate established security policy or procedures.

j. Cooperating with the Inspection Service to ensure the physical protection of the network infrastructure located at the facility.

k. Developing, maintaining, and testing:

   (1) Emergency Action Plans required for each facility to ensure personnel are safely evacuated and provides for the protection of the employees.

   (2) Incident Management Facility Recovery Plan required for each major IT site.

   (3) Workgroup Recovery Plan required for each business function.

   (4) Disaster Recovery Plan (DRP) (business information systems disaster) documents required for each critical system that supports essential (core) business functions.

l. Implementing and managing the following plans and team members:

   (1) Emergency Action Plan.

   (2) Incident Management Facility Recovery Plan.

   (3) Workgroup Recovery and “Beyond” Continuity of Operations (COOP) Plans.

   (4) DRP (business information systems disaster) documents.

m. Reporting information security incidents to the CIRT in a timely manner, containing the incident, following continuity plans for disruptive incidents, and assessing damage caused by the incident.

2-2.14 Chief Privacy Officer

The CPO is responsible for the following:

a. Developing policy for defining information sensitivity and determining information sensitivity designations.

b. Providing guidance on privacy issues to ensure Postal Service compliance with the Privacy Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, and Freedom of Information Act.

c. Developing privacy compliance standards, customer privacy statement, and customer data collection standards, including cookies and Web-transfer notifications.

d. Developing appropriate data record retention, disposal, and release procedures and standards.

e. Approving requests for message and data content monitoring.

f. Consulting on and reviewing the BIA and approving the determination of information sensitivity.

2-2.15 Inspector General

The inspector general is responsible for the following:

a. Conducting independent financial audits and evaluation of the operation of the Postal Service to ensure that its assets and resources are fully protected.

b. Preventing, detecting, and reporting fraud, waste, and program abuse.

c. Promoting efficiency in the operation of the Postal Service.

d. Funding CISO investigative efforts outside of those normally required.

e. The manager, Technical Crimes Unit, is responsible for the following:

(1) Functioning as an ongoing liaison with the CIRT.

(2) Serving as a point of contact between the CIRT and law enforcement agencies.

(3) Conducting criminal investigations of attacks upon Postal Service networks and computers.

2-2.16 Manager, Business Continuance Management

The manager, Business Continuance Management, is responsible for the following:

a. Protecting the health and safety of Postal Service employees.

b. Ensuring the continuity of business, expediting recovery from a loss of a single critical system or a major disruption to business functions.

c. Reviewing and assessing Business Continuity Management (BCM) program plans.

d. Defining, planning, developing, implementing, managing, assuring the testing and exercising, and monitoring for compliance of a sustainable BCM program for the Postal Service.

e. Ensuring appropriate Business Continuity Plans (BCPs) are developed, tested, and exercised for business functions and information technology services.

f. Ensuring appropriate DRP documents are developed and business information systems are tested for all critical and business functions and services.

g. Certifying all DRP test and BCP exercise.

h. Developing and implementing lines of communication to the IT organization about BCM matters.

i. Promoting BCM awareness and providing training for Postal Service personnel.

j. Ensuring compliance with BCM and information security policies.

k. Establishing BCM policy and strategy.

2-2.17 Manager, Telecommunications Services

The manager, Telecommunications Services (TS), is responsible for the following:

a. Implementing and maintaining operational information security throughout the network infrastructure including timely security patch management.

b. Recommending and deploying network hardware and software based on the Postal Service security architecture.

c. Operational monitoring and tracking of all physical connections between any component of the Postal Service telecommunications infrastructure and any associated information resource not under Postal Service control.

d. Implementing security controls and processes to safeguard the availability and integrity of the Postal Service intranet including physical access to network infrastructure and the confidentiality of sensitive-enhanced and sensitive information.

e. Implementing the network perimeter firewalls, demilitarized zones, secure enclaves, and proxy servers.

f. Designating TS representative(s) to the NCRB.

g. Ensuring secure and appropriate connectivity to the Postal Service intranet.

h. Ensuring network services and protocols used by Postal Service information resources provide the appropriate level of security for the Postal Service intranet and the information transmitted.

i. Implementing secure methods of remote access and appropriate remote access controls.

j. Implementing two-factor authentication and the associated infrastructure for network management.

k. Implementing only Postal Service-approved encryption technology.

l. Implementing appropriate network security administration and managing accounts appropriately.

m. Maintaining the integrity of data and network information resources.

n. Supporting the implementation of approved security incident detection and prevention technologies (e.g., virus scanning, intrusion detection systems, and intrusion prevention systems) throughout the perimeter.

o. Maintaining an accurate inventory of Postal Service network information resources.

p. Monitoring network security alerts and logs and providing network security audit logs to the CISO ISS.

q. Ensuring that recovery plans and sufficient capacity are in place for the recovery of the telecommunications infrastructure for the IT-supported Postal Service sites.

r. Identifying and training key technical personnel to provide support in BCM for information resources housed in IT-supported Postal Service sites.

s. Monitoring network traffic for anomalies, conducting perimeter scanning for viruses, malicious code, and usage of nonstandard network protocols, and immediately reporting suspected information security incidents to the CIRT.

t. Protecting information resources at risk during security incidents (if feasible) and providing support for CIRT incident containment and response.

u. Implementing and managing wireless local area network connectivity.

2-2.18 Managers Responsible for Computing Operations

The managers responsible for computing operations are responsible for the following:

a. Implementing information security policies, procedures, and standards and ensuring compliance.

b. Coordinating and implementing standard platform configurations based on the Postal Service security architecture.

c. Creating and maintaining a timely patch management process and deploying patches to resources under their control.

d. Maintaining an accurate inventory of Postal Service information resources, tracking and reacting to security vulnerability alerts, coordinating hardware and software upgrades, and maintaining appropriate records.

e. Deploying and maintaining anti-virus software and recognition patterns to scan for malicious code and usage of nonstandard network protocols.

f. Supporting the C&A process for internally managed information resources.

g. Ensuring that remote access is appropriately managed.

h. Implementing appropriate security administration and ensuring that accounts are managed appropriately.

i. Maintaining the integrity of data and information resources and ensuring the appropriate level of information resource availability.

j. Ensuring the installation of the authorized internal warning banner (see Exhibit 14-3.3).

k. Disseminating security awareness and warning advisories to local users.

l. Reporting suspected information security incidents to the CIRT in a timely manner, protecting information resources at risk during security incidents, implementing containment, and assisting in restoring information resources following an attack.

2-2.19 Managers of Development Centers

Managers of development centers are responsible for the following:

a. Ensuring developers are trained in the Postal Service technical solutions life cycle and secure coding techniques.

b. Providing support services to the executive sponsor through the appropriate portfolio manager for all matters relating to BCM.

c. Ensuring that continuity plans are developed for information resource developed at their site or information resource developed under their governance and that those plans are tested in accordance with the information resource's designated criticality.

d. Identifying and training key technical personnel to provide support for testing continuity plans for their facility and for critical information resources developed at their site or under their governance, for critical information resources housed at their site or alternate site facilities, and for off-site support of critical information resources in case of disaster.

2-2.20 Manager, Corporate Information Security Office Information Systems Security

The manager, CISO ISS is responsible for the following:

a. Determining the requirements and standards for secure enclaves.

b. Assessing information resources to determine the need for placement in a secure enclave.

c. Recommending and approving standard configurations and hardening standards for Postal Service information resources.

d. Approving two-factor authentication (e.g., digital certificates, digital signatures, biometrics, smart cards, and tokens) and the associated infrastructure for network management.

e. Approving and managing intrusion detection systems and intrusion prevention systems.

f. Approving, managing, and ensuring appropriate perimeter penetration testing and network vulnerability scans and testing.

g. Providing support to the OIG during the conduct of investigative activities concerning information security, the computing infrastructures, and network intrusion as requested.

h. Approving the use of networking monitoring tools, except those used by the OIG.

i. Providing support to the chief inspector during his or her conduct of site security reviews as requested.

j. Conducting monitoring and surveillance activities.

k. Collecting, correlating, and reviewing all Postal Service security audit log files.

l. Reviewing information security policy and processes for MPE/MHE.

m. Developing and maintaining an information security architecture and coordinating a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.

n. Removing network connectivity from any computing device that does not meet the defined operating system and anti-virus software and recognition pattern thresholds.

o. Managing the NCRB to control connectivity to the Postal Service computing infrastructure.

p. Designating the chairperson of the NCRB and additional ISS representative(s) to the NCRB, as required.

q. The NCRB is responsible for the following:

(1) Managing the Postal Service network connectivity process through the implementation of the Information Security Network Connectivity Process.

(2) Developing system connectivity requirements for Postal Service connections to external systems, externally facing information resources (e.g., FTP servers), and connections via the Internet to Postal Service development, production, and internal networks.

(3) Developing standard connectivity and documentation criteria to expedite approval of connectivity requests without additional board action.

(4) Requesting additional information, security reviews, or audits about proposed or approved connections, if deemed necessary.

(5) Evaluating connectivity and firewall change requests and approving or rejecting them based upon existing policy, best practices, and the level of risk associated with the request.

(6) Consulting with executive sponsors on network information security requirements.

(7) Assisting the requester in identifying alternative solutions for denied requests that are acceptable to the requester and the Postal Service.

(8) Reviewing new information resource, infrastructure, and network connections and their effects on overall Postal Service operations and information security.

(9) Recommending and approving network services and protocols.

(10) Recommending changes to the business partner network. In situations where high-risk factors exist, issuing mitigating requirements for connectivity.

(11) Ordering the disabling of an information resource or network connection that does not comply with Postal Service policies, procedures, and standards or which is found to pose a significantly greater risk than when originally assessed.

r. Managing the CIRT to help the Postal Service contain, eradicate, document, and recover following a computer security incident and return to a normal operating state.

s. The CIRT is responsible for the following:

(1) Providing timely and effective response to computer security incidents as they occur.

(2) Working with an organization to contain, eradicate, document, and recover following a computer security incident.

(3) Engaging other Postal Service organizations including, but not limited to, the OIG and Inspection Service.

(4) Escalating information security issues to executive management as required.

(5) Conducting a post-incident analysis, where appropriate, and recommending preventive actions.

(6) Maintaining a repository for documenting, analyzing, and tracking Postal Service security incidents until they are closed.

(7) Interfacing with other governmental agencies and private-sector computer incident response centers.

(8) Participating in and providing information for Postal Service security awareness.

(9) Developing and documenting processes for incident reporting and management.

(10) Providing support to the OIG and the Inspection Service, as requested.

2-2.21 Managers, Help Desks

The managers, Help Desks, are responsible for the following:

a. Creating the entry for the problem tracking management system for security incidents reported to the Help Desks.

b. Providing technical assistance for responding to suspected virus incidents reported to the Help Desks.

c. Escalating unresolved suspected virus events to the CIRT.

2-2.22 Contracting Officers and Contracting Officer Representatives

Contracting officers, contracting officer representatives, and employees approving nonsupply management contracts are responsible for the following:

a. Ensuring that information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.

b. Ensuring that all contracts and business agreements requiring access to Postal Service information resources identify sensitive positions, specify the clearance levels required for the work, and address appropriate security requirements.

c. Ensuring that contracts and business agreements allow monitoring and auditing of any information resource project.

d. Ensuring that the security provisions of the contract and business agreements are met.

e. Confirming the employment status and clearance of all contractors who request access to information resources.

f. Ensuring all account references, building access, and other privileges are removed for contractor personnel when they are transferred or terminated.

2-2.23 General Counsel

The general counsel is responsible for the following:

a. Ensuring that information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.

b. Ensuring that contracts and agreements allow monitoring and auditing of Postal Service information resource projects.

2-2.24 Business Partners

Business partners may request connectivity to Postal Service network facilities for legitimate business needs. Business partners requesting or using connectivity to Postal Service network facilities are responsible for the following:

a. Initiating a request for connectivity to the Postal Service executive who sponsors the request.

b. Complying with Postal Service network connectivity request (see Handbook AS-805-D*, Information Security Network Connectivity Process)* requirements and process.

c. Abiding by Postal Service information security policies regardless of where the systems are located or who operates them. This also includes strategic alliances.

d. Protecting information resources at risk during security incidents, if feasible.

e. Reporting information security incidents promptly to the CIRT, the executive sponsor, and the information systems security officer (ISSO) assigned to their project.

f. Taking action, as directed by the CIRT, to eradicate the incident, recover from it, and document actions regarding the security incident.

g. Allowing site security reviews by the Postal Inspection Service and CISO.

h. Allowing audits by the OIG.

2-2.25 Accreditor

The manager, CISO, functions as the accreditor and is responsible for the following:

a. Reviewing the risk mitigation plan and supporting C&A documentation package together with business requirements and relevant Postal Service issues.

b. Escalating security concerns or preparing and signing an accreditation letter that makes one of the following recommendations: accepting the information resource with its existing information security controls, requiring additional security controls with a timeline to implement, or deferring deployment until information security requirements can be met.

c. Forwarding the accreditation letter and C&A documentation package to the portfolio manager and executive sponsor.

2-2.26 Certifier

The program manager, Security Certification and Accreditation Process, who is appointed by the manager, CISO, functions as the certifier and is responsible for the following:

a. Managing and providing guidance to the ISSOs.

b. Reviewing the C&A evaluation report and the supporting C&A documentation package.

c. Escalating security concerns or preparing and signing a certification letter.

d. Forwarding the certification letter and C&A documentation package to the portfolio manager.

e. Maintaining an inventory of all information resources that have completed the C&A process.

2-2.27 Security Control Officers

SCOs ensure the general security of the facilities to which they are appointed, including the safety of on-duty personnel and the security of mail, Postal Service funds, property, and records entrusted to them [see the *Administrative Support Manual* (ASM) 271.3, Security Control Officers]. SCOs are responsible for the following:

a. Establishing and maintaining overall physical and environmental security at the facility, with technical guidance from the Inspection Service.

b. Establishing controlled areas within the facility, where required, to protect information resources designated as sensitive-enhanced, sensitive, or critical.

c. Establishing and maintaining access control lists of people who are authorized access to specific controlled areas within the facility.

d. Ensuring positive identification and control of all personnel and visitors in the facility.

e. Ensuring the protection of servers, workstations, portable devices, and information located at the facility.

f. Consulting on the facility COOP plans.

g. Conducting annual facility security reviews using the site security survey provided by the Inspection Service.

h. Reporting suspected information security incidents to the CIRT and providing support for incident containment and response, as requested.

i. Responding to physical security incidents and reporting physical security incidents to the Inspection Service.

j. Interfacing with CIRT, Inspection Service, CISO, or OIG, as required.

2-2.28 Information Systems Security Representatives

ISSRs are appointed in writing by the executive sponsors or the portfolio manager and are members of the information resource development or integration teams. The role of the ISSR can be an ad hoc responsibility performed in conjunction with assigned duties. The project manager often performs the role of the ISSR. ISSRs are responsible for the following:

a. Providing support to the executive sponsor and portfolio manager, as required.

b. Promoting information security awareness on the project team.

c. Ensuring security controls and processes are implemented.

d. Notifying the executive sponsor, portfolio manager, and ISSO of any additional security risks or concerns that emerge during development or acquisition of the information resource.

e. Developing or reviewing security-related documents required by the C&A process as assigned by the executive sponsor or portfolio manager.

f. Organizing the C&A documentation package and forwarding the package to the ISSO.

2-2.29 Information Systems Security Officers

ISSOs are responsible for the following:

a. Chairing the C&A team.

b. Ensuring that a BIA is completed for each information resource.

c. Ensuring that the responsible project manager records the sensitivity and criticality designations in EIR.

d. Advising and consulting with executive sponsors and portfolio managers during the BIA process so they know the background for (1) baseline security requirements that apply to all information resources and (2) the security requirements necessary to protect an information resource based on the resource's sensitivity and criticality designation.

e. Recommending security requirements to executive sponsors and portfolio managers during the BIA process, based on generally accepted industry practices and the risks associated with the information resource.

f. Providing guidance on how information resources are vulnerable to threats, what controls and countermeasures are appropriate, and the C&A process.

g. Conducting site security reviews or helping the Inspection Service conduct them.

h. Reviewing the C&A documentation package.

i. Preparing and signing the C&A evaluation report and forwarding the evaluation report and C&A documentation to the certifier.

2-2.30 System Administrators

System administrators are technical personnel who serve as computer systems, network, and firewall administrators, whether the system management function is centralized, distributed, subcontracted, or outsourced. System administrators are responsible for the following:

a. Implementing information security policies and procedures for all information resources under their control, and also for monitoring the implementation for proper functioning of security mechanisms.

b. Implementing appropriate platform security based on the platform-specific hardening standards for the information resources under their control.

c. Complying with standard configuration settings, services, protocols, and change control procedures.

d. Applying approved patches and modifications in accordance with policies and procedures established by the Postal Service. Ensuring that security patches and bug fixes are kept current for resources under their control.

e. Implementing appropriate security administration and ensuring that logon IDs are unique.

f. Setting up and managing accounts for information resources under their control in accordance with policies and procedures established by the Postal Service.

g. Disabling accounts of personnel whose employment has been terminated, who have been transferred, or whose accounts have been inactive for an extended period of time.

h. Making the final disposition (e.g., deletion) of the accounts and the information stored under those accounts.

i. Managing sessions and authentication and implementing account time-outs.

j. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.

k. Testing information resources to ensure security mechanisms are functioning properly.

l. Tracking hardware and software vulnerabilities.

m. Maintaining an accurate inventory of Postal Service information resources under their control.

n. Ensuring that audit and operational logs, as appropriate for the specific platform, are implemented, monitored, protected from unauthorized disclosure or modification, and are retained for the time period specified by Postal Service security policy.

o. Reviewing audit and operational logs and maintaining records of the reviews.

p. Identifying anomalies and possible internal and external attacks on Postal Service information resources.

q. Reporting information security incidents and anomalies to their manager and the CIRT immediately upon detecting or receiving notice of a security incident.

r. Protecting information resources at risk during security incidents, assisting in the containment of security incidents as required, and taking action as directed by the CIRT.

s. Participating in follow-up calls with the CIRT and fixing issues identified following an incident.

t. Ensuring that virus protection software and signature files are updated and kept current for resources under their control.

u. Ensuring the availability of information resources by implementing backup and recovery procedures.

v. v. Ensuring the compliance with Postal Service information security policy and procedures.

w. Monitoring the implementation of network security mechanisms to ensure that they are functioning properly and are in compliance with established security policies.

x. Maintaining a record of all monitoring activities for information resources under their control.

y. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.

2-2.31 Database Administrators

Database administrators (DBAs) are responsible for the following:

a. Implementing appropriate database security based on the platform-specific hardening standards for the information resources under their control.

b. Implementing information security policies and procedures for all database platforms and monitoring the implementation of database security mechanisms to ensure that they are functioning properly and are in compliance with established policies.

c. Applying approved patches and modifications, in accordance with policies and procedures established by the Postal Service.

d. Maintaining an accurate inventory of Postal Service information resources under their control.

e. Implementing appropriate database security administration and ensuring that logon IDs are unique.

f. Setting up and managing accounts for systems under their control in accordance with policies and procedures established by the Postal Service.

g. Disabling accounts of personnel that have been terminated, transferred, or have accounts that have been inactive for an extended period of time.

h. Making the final disposition (e.g., deletion) of the accounts and the information stored under those accounts.

i. Managing sessions and authentication and implementing account time-outs.

j. Preventing residual data from exposure to unauthorized users as information resources are released or reallocated.

k. Testing database software to ensure that security mechanisms are functioning properly.

l. Tracking database software vulnerabilities, and deploying database security patches.

m. Ensuring database logs are turned on, logging appropriate information, protected from unauthorized disclosure or modification, and retained for the time period specified.

n. Reviewing database audit logs and maintaining records of log reviews.

o. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.

p. Ensuring the availability of databases by implementing database backup and recovery procedures.

q. Identifying anomalies and possible attacks on Postal Service information resources.

r. Reporting information security incidents and anomalies to their manager and the CIRT immediately upon detecting or receiving notice of a security incident.

s. Protecting information resources at risk during security incidents, assisting in the containment of security incidents as required, and taking action as directed by the CIRT.

2-2.32 All Personnel

All personnel, including employees, consultants, subcontractors, business partners, customers who access nonpublicly available Postal Service information resources (e.g., mainframes or the internal Postal Service network), and other authorized users of Postal Service information resources are responsible for the following:

a. Complying with applicable laws, regulations, and Postal Service information security policies, standards, and procedures.

b. Displaying proper identification while in any facility that provides access to Postal Service information resources.

c. Being aware of their physical surroundings, including weaknesses in physical security and the presence of any authorized or unauthorized visitor.

d. Protecting information resources, including workstations, portable devices, information, and media.

e. Always using their physical and technology electromechanical access control identification badge or device to gain entrance to a controlled area.

f. Ensuring no one tailgates into a controlled area on their badge.

g. Performing the security functions and duties associated with their job, including the safeguarding of their logon IDs and passwords.

h. Changing their password immediately, if they suspect that the password has been compromised.

i. Prohibiting any use of their accounts, logon IDs, passwords, personal information numbers (PINs), and tokens by another individual.

j. Taking immediate action to protect the information resources at risk upon discovering a security deficiency or violation.

k. Only using licensed and approved hardware and software.

l. Protecting intellectual property.

m. Complying with Postal Service remote access information security policies, including those for virtual private networks, modem access, dial-in access, secure telecommuting, and remote management and maintenance.

n. Complying with acceptable use policies.

o. Maintaining an accurate inventory of information resources for which they are responsible.

p. Protecting information resources against viruses and malicious code.

q. Calling the appropriate Help Desk for technical assistance in response to suspected virus incidents.

r. Promptly reporting to the CIRT and, as appropriate, to their immediate supervisor, manager, or system administrator, any suspected security incidents, including security violations or suspicious actions, suspicion or occurrence of any fraudulent activity; unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information; and potentially dangerous activities or conditions.

s. Taking action, as directed by the CIRT, to protect against information security incidents, to contain and eradicate them when they occur, and to recover from them.

t. Documenting all conversations and actions regarding the security incident and completing PS Form 1360, *Information Security Incident Report,* or an acceptable facsimile.

u. If an employee removes a portable electronic device from a Postal Service facility, he or she must do the following:

(1) If the device contains sensitive-enhanced or sensitive information, request approval in writing from his or her functional area vice president (data steward) and the VP IT Operations or their designees.

(2) Protect the device and the data it contains.

(3) Keep the device within sight, secured with a cable lock, or locked in a cabinet or closet.

(4) Do not check the device in baggage on an airplane, train, or any other public transportation.

(5) If her or she must leave the device in his or her vehicle, keep the device out of sight in the trunk. Never leave the device in a vehicle overnight.

(6) Encrypt sensitive-enhanced and sensitive data on the hard drive, flash drive, or other removable media. If in doubt, encrypt using WinZip, Encryption File System (EFS), or an encryptable flash drive.

v. Report any missing or stolen device or media immediately to his or her manager, the CIRT via e-mail to *uspscirt@usps.gov,* and to the local Inspection Service office. If the device has been stolen somewhere other than Postal Service premises, report the theft to the local police as well.

This page intentionally left blank

3 Information Designation and Control

3-1 Policy

Information resources are strategic assets vital to the business performance of the Postal Service. These strategic assets belong to the Postal Service as an organization and not to any individual or group of individuals and must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Postal Service's ability to conduct its mission.

Postal Service information resources must be protected from time of capture to retirement, disposal, and destruction commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Postal Service's ability to conduct its mission.

All personnel must implement the protection requirements defined in the following areas: information designation, categorization, and protection (including labeling, handling, controlling access and retention, protecting in transit and in storage, disposal, and destruction). Furthermore, Postal Service information resources must be configured to comply with Postal Service data stewardship policies.

Chapter 3 addresses the following:

a. Information designation and categorization.
b. Determination of the categorization of information resources.
c. Security requirements categories.
d. Protection of Postal Service information and media.
e. Protection of non-Postal Service information.

3-2 Information Designation and Categorization

Information at the Postal Service is designated and categorized based on the classification, sensitivity, and criticality of the information.

3-2.1 Designation Categories and Levels

Classification, sensitivity, and criticality designation categories and levels are defined in Exhibit 3-2.1.

Exhibit 3-2.1
Designation Categories and Levels

Designation Category	Description	Levels *(In decreasing order of necessity to protect the confidentiality, integrity, and availability of the information)*
Classified	Classification levels determine the need to protect the confidentiality and integrity of classified information.	Top Secret Secret Confidential Unclassified Information
Sensitive	Sensitivity determines the need to protect the confidentiality and integrity of sensitive information.	Sensitive-Enhanced Unclassified Information (hereafter referred to as Sensitive-Enhanced) Sensitive Unclassified Information (hereafter referred to as Sensitive) Nonsensitive Unclassified Information (hereafter referred to as Nonsensitive)
Critical	Criticality reflects the need for continuous availability of the information.	Critical Noncritical

3-2.2 Sensitivity and Criticality Category Independence

Sensitivity and criticality are independent designations. All Postal Service information must be evaluated to determine both sensitivity and criticality. Information with any sensitivity level may have any level of criticality level and vice versa.

3-2.3 Definitions of Classified, Sensitive, and Critical Information

3-2.3.1 Classified Information

Classified information is hardcopy or electronic information or material that has been designated as classified pursuant to executive order, statue, or regulation and requires protection against unauthorized disclosure for reasons of national security. National security reasons includes national defense, foreign relations of the United States, intelligence activities, atomic weapons and special nuclear material, crypto logic activities related to national security, command and control of military forces, integral components of weapon systems, or critical to direct fulfillment of military or intelligence missions. Classified designations include Confidential, Secret, and Top Secret. Categories of classified information include restricted data (RD), formerly restricted data (FRD), and national security information (NSI).

Note: Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

3-2.3.2 Sensitive-Enhanced Information

Sensitive-enhanced information is hardcopy or electronic information or material that is not designated as classified but that warrants or requires

enhanced protection. Requirements to protect sensitive-enhanced information are derived from law, regulation, the law enforcement and judicial process, the payment card industry (PCI), and the Privacy Act of 1974 as amended. Types of sensitive-enhanced information include:

- Law enforcement information and court-restricted information, including grand jury material, arrest records, and information about ongoing investigations.
- PCI cardholder information.
- Personal identifiers (e.g., identify individuals in a recognizable form including social security numbers, driver license numbers, passport number, fingerprints, and other biometric information) and 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).

3-2.3.3 Sensitive Information

Sensitive information is hardcopy or electronic information or material that is not designated as classified or sensitive-enhanced but that warrants or requires protection. Requirements to protect sensitive information are derived from law, regulation, the Privacy Act of 1974 as amended, business needs, and the contracting process. Types of sensitive information include:

- 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 such as physical, technical or network/DMZ/enclave/ mainframe/server/workstation specifics including security settings, passwords, audit logs.

3-2.3.4 Nonsensitive Information

Information that is not designated as classified, sensitive-enhanced, or sensitive information is by default designated as nonsensitive information. An example is publicly available information. Even though information is

designated as nonsensitive information, it must still be protected (i.e., baseline requirements apply to all Postal Service information).

3-2.3.5 Critical Information

Information is designated as critical information if its unavailability would have a significant negative impact on customer or employee life, safety, or health; paying suppliers or employees; collecting revenue; movement of mail; communications; and infrastructure services.

3-2.3.6 Noncritical Information

Information that is not designated as critical is by default designated as noncritical.

3-3 Determination of the Categorization of Information Resources

3-3.1 Business Impact Assessment

The Business Impact Assessment (BIA) is a process for determining the categorization of Postal Service information resources. A BIA must be completed for all information resources, whether the information resource is developed in house, outsourced or hosted in non-Postal Service facilities. The BIA must be updated periodically as required (every one, three, or five years depending on its sensitivity designation), whenever a significant change is made to the information resource, or whenever the certification and accreditation (C&A) process is re-initiated.

Various stakeholders [e.g., management, operational personnel, and information systems security officers (ISSOs)] need to be involved in the BIA process. An information resource may process several information types. Each information type is subject to security categorization. The stakeholders must consider the consequences of unauthorized disclosure of privacy information with respect to violations of federal policy and law. The impact of privacy violations will depend in part on the penalties associated with violation of the relevant statutes and policies. A privacy impact assessment (PIA) is included in the BIA.

The impact level for an information resource will normally be the highest impact level for the following security objectives associated with the information types:

a. Confidentiality — Preserving authorized restrictions on information access and disclosure.

b. Integrity — Guarding against improper information modification or destruction.

c. Availability — Ensuring timely and reliable access to information.

However in some cases, the security category for a system may be higher than any impact level for any information type processed by the system. Variations in sensitivity/criticality with respect to time may also need to be factored into the impact assignment process. Some information loses its

sensitivity in time (e.g., a Postal Service rate increase becomes nonsensitive after it has been published). Some applications are particularly critical at some point in time (e.g., the payroll application on the day for normal processing).

3-3.1.1 Aggregation

Some information may have little or no sensitivity in isolation but may have high sensitivity in aggregate. In some cases, aggregation of large quantities of a single information type can reveal patterns and/or plans, or facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous information types can have similar effects. In general, the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of a bank account number with the identity of an individual and/or institution).

The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system categorization may need to be adjusted to a higher level than would be indicated by the impact associated with any individual information type.

3-3.1.2 System Functionality

Compromise of some information types may have low impact in the context of a system's primary function but may have much more significance when viewed in the context of the potential impact of compromising:

a. Other systems to which the system in question is connected, or

b. Other systems which are dependent on that system's information.

Access control information for a system that processes only low-impact information might initially be thought to have only low-impact attributes. However, if access to that system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered.

Similarly, some information may, in general, have low-sensitivity or criticality attributes. However, that information may be used by other systems to enable sensitive-enhanced, sensitive, or critical functions. Loss of data integrity, availability, temporal context, or other context can have severe consequences.

3-3.1.3 Critical National Infrastructure

Where the mission served by an information system, or the information that the system processes affects the security of the critical national infrastructure, the loss of confidentiality, integrity, or availability could result in a higher designation.

3-3.2 Approving Information Resource Classification and Categories of Information Processed

The determination of the sensitivity for each information resource and the categories of information processed must be approved by the chief privacy officer or his or her designee through the BIA. The determination of the criticality for each information resource must be approved by the postmaster general and his senior executives. This process is facilitated by the manager of Business Continuance Management or his or her designee.

3-3.3 Recording Information Resource Classification and Categories of Information Processed

The sensitivity and criticality for each information resource and the categories of information processed must be documented in the Enterprise Information Repository (EIR) and in the information security plan.

3-4 Security Requirement Categories

The Postal Service uses several categories of security requirements to protect information resources (see Exhibit 3-4).

A security requirement is a type or level of protection that secures an information resource. A control consists of safeguards designed to respond to a security requirement. A control may satisfy more than one requirement, or several controls may be needed to satisfy a security requirement depending on the sensitivity and criticality of the information resource and its operating environment. If a requirement cannot be addressed, compensating controls can be implemented to mitigate the risk.

Exhibit 3-4
Security Requirement Categories

Security Requirement Category	Control(s)
Baseline	All information resources must implement controls sufficient to satisfy the baseline security requirements. Baseline security requirements have been established to protect the Postal Service computing environment and infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction.
Sensitive-Enhanced, Sensitive, PCI, Law Enforcement, and Critical	Additional security is needed to adequately protect sensitive-enhanced, sensitive, and critical information resources. These requirements are based on the following: Sensitivity and criticality of the information resource. Federal legislation [e.g., the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act. Federal regulations (e.g., requirements for cryptographic modules). Federal directives (e.g., personal identity verification and critical infrastructure). Industry requirements (e.g., PCI).
Conditional	Requirements requested by the chief information officer, vice president, Information Technology Operations; manager CISO; or the functional VP or requirements based on specific criteria such as the development and operating environment.

Security Requirement Category	Control(s)
Recommended	ISSOs may recommend additional security requirements during the BIA process to better protect the information resource against threats and vulnerabilities. Recommended security requirements are based on generally accepted industry practices. The executive sponsor assumes the risks associated with not implementing the recommended security requirements.

3-5 Protection of Postal Service Information and Media

All Postal Service information must be properly handled and controlled based on the information sensitivity and criticality. Labeling, retention, storage, encryption, release, and destruction of information must comply with established Postal Service policies and procedures specified below and in Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management.* Postal Service policies address the following:

a. Labeling of information and media.
b. Controlling access to information.
c. Retention and storage of information.
d. Encryption of information.
e. Removal of Postal Service information from Postal Service premises.
f. Release of information.
g. Handling contaminated information resources.
h. Disposal and destruction of information and media.

3-5.1 Labeling of Information and Media

3-5.1.1 Electronic Media and Hardcopy Output

Electronic media [e.g., disks, diskettes, tapes, and universal serial bus (USB) storage devices] and hardcopy output (e.g., printouts, screen prints, photocopies, architecture drawings, and engineering layouts) which contain sensitive-enhanced or sensitive information must be legibly and durably labeled as “RESTRICTED INFORMATION.”

3-5.1.2 Applications Processing

On applications processing sensitive-enhanced or sensitive information, the following statement must be prominently displayed on the login/password screen or the welcome screen: “Information within this application is designated sensitive-enhanced (or sensitive) and should be properly protected from unauthorized access or disclosure.” Additionally, the “Print Screen” function can also result in hardcopy that must be legibly and durably labeled as “RESTRICTED INFORMATION.”

3-5.2 Controlling Access to Information

Access to information in hardcopy and digital form must be restricted to authorized personnel as follows:

a. To prevent unauthorized access to hardcopy and electronic media, any of the following controls may be employed:
   (1) A locked desk or file cabinet.
   (2) A room with a key, combination, or electronic lock.
   (3) An approved media storage area or an area behind a guard.

b. To prevent unauthorized access to electronic files and databases, access controls must be employed. Access attempts granted and refused are subject to audit.

c. Sensitive-enhanced and sensitive information must be protected from unauthorized access and disclosure. Access must be restricted to authorized personnel with a need to know. Metadata (i.e., data describing the structure, content, and context of electronic information) must also be protected from unauthorized access and disclosure.

d. Critical information must be protected from unauthorized access and destruction.

3-5.3 Retention and Storage of Information

The retention and storage of information must be controlled as follows:

a. All Postal Service information must be retained in accordance with legal retention requirements established by law (e.g., legal holds), and also with operational retention requirements established by the Postal Service Records Office (see Handbook AS-353).

b. When the retention period or legal hold has expired, sensitive-enhanced, sensitive, and critical information must be properly destroyed as described in 3-5.8, Disposal and Destruction of Information and Media, of this handbook. The process of removing expired information can be automated or manual.

c. Sensitive-enhanced, sensitive, and critical information must be stored only on Postal Service-owned devices, in a controlled area or a locked cabinet in accordance with established Postal Service policies and procedures.

d. Nonpublicly available Postal Service information must be isolated and stored separately from non-Postal Service information (e.g., business partner and vendor information) unless required by law or regulation. Nonpublicly available Postal Service information and non-Postal Service information must be stored separately at Postal Service facilities, non-Postal Service facilities, or at backup sites unless required by law or regulation.

3-5.4 Encryption of Information

Examples of conditions under which Postal Service information must be encrypted include, but are not limited to, the following:

a. Sensitive-enhanced and sensitive information in transit across networks.

b. Sensitive-enhanced and sensitive information at rest including stored or archived on removable devices or media including disks, diskettes, CDs, and USB storage devices.

c. Sensitive-enhanced and sensitive information that is stored off Postal Service premises.

d. PCI information (encrypted throughout the life cycle).

3-5.5 Removal of Postal Service Information from Postal Service Premises

The requirements for (1) accessing or downloading sensitive-enhanced and sensitive Postal Service electronic information off Postal Service premises or (2) taking sensitive-enhanced and sensitive Postal Service electronic and nonelectronic information off site (i.e., non-Postal Service premises) including Postal Service data processed by business partners are:

a. The removal and storage of sensitive-enhanced and sensitive Postal Service electronic information from Postal Service premises must be approved in writing by the functional vice president (data steward) and the CIO or their designee. Complete PS Form 1357-D, *Data Accountability,* to initiate the process.

b. Only authorized personnel are allowed to pick up, receive, transfer, or deliver Postal Service sensitive-enhanced and sensitive information.

c. Postal Service information accessed, processed, or stored at non-Postal Service sites must be encrypted and processed on Postal Service-owned hardware and software. The use of business partner hardware and software must be approved by the functional vice president (data steward) and the CIO or their designee. The use of business partner hardware and software must also meet Postal Service standards for server hardening and malicious code protection and will be subject to unannounced audit.

d. ACE-supported infrastructure components must connect to the Postal Service intranet over a secure link at least weekly to receive appropriate security patches and virus recognition patterns. Non-ACE-supported infrastructure components must be appropriately patched and have the latest virus recognition patterns installed.

e. All Postal Service sensitive-enhanced and sensitive information must be encrypted during transmission, in storage on removable media and mobile devices. Also, all sensitive-enhanced and sensitive information must be encrypted in storage off Postal Service premises. Cardholder information must not be stored off Postal Service premises on hard drives, removable devices, or media.

f. All Postal Service hardware devices, hardcopy, and media (including backups) containing sensitive-enhanced and sensitive information must be secured against theft and unauthorized access (e.g., controlled area, safe, and locked cabinet). Approved business partner devices must be likewise secured.

g. There must be accountability in the life cycle management of any sensitive-enhanced and sensitive information removed off Postal Service premises. This data and all copies must be inventoried annually and formally tracked (e.g., logbook and tape management system) from creation to destruction.

3-5.6 Release of Information

The release of information must be accomplished in accordance with Postal Service policies and procedures (see Handbook AS-353).

Sensitive-enhanced and sensitive information must be protected from unauthorized disclosure, whether formally or informally through conversations, e-mail, voice, facsimile, and observed workstation screens.

3-5.6.1 Releasing Information on Factory-Fresh or Degaussed Media

Before releasing information on electronic media outside the Postal Service, the information must be copied onto factory-fresh media (never used) or onto media that was appropriately degaussed to prevent inadvertent release of sensitive-enhanced and sensitive information.

3-5.6.2 Precautions Prior to Maintenance

To prevent inadvertent disclosure of sensitive-enhanced and sensitive information, all hardware and electronic media being released for maintenance outside of Postal Service facilities must, prior to release, undergo data eradication according to approved Postal Service procedures. If electronic media containing sensitive-enhanced and sensitive information is released to a contractor or vendor for maintenance, the Postal Service must have in place a legally binding contract regarding the secure handling and storage of the data or media.

3-5.7 Handling Biohazard Contaminated Information Resources

3-5.7.1 Sensitive-Enhanced and Sensitive Information

Any personnel handling biohazard contaminated Postal Service information resources must follow the standards set forth by the Inspection Service for handling contaminated devices. If the contaminated information resource contains sensitive-enhanced and sensitive information, the Inspection Service must be notified regarding the type of device, the classification of data it contains (i.e., sensitive-enhanced or sensitive), and the Postal Service manager responsible for the device. Disposition of the contaminated information resource must be recorded, including who took possession of the device and the disposition expected for the resource.

3-5.7.2 Data Eradication on Contaminated Information Resources

Any Postal Service hardware or electronic media being released outside of Postal Service facilities must, prior to release, undergo data eradication, if possible, according to approved Postal Service procedures. Eradication procedures may include the ability to eradicate data through remote management of the information resource. If data eradication is not possible, the Inspection Service must be advised and notification must be made to all persons involved in the chain of possession of their responsibility for nondisclosure of the information contained in the device. It is strongly recommended that a memorandum of nondisclosure be signed by all personnel involved in the chain of possession of the contaminated information resource.

3-5.7.3 Reporting of Contaminated Information Resources

The Postal Service manager responsible for the contaminated device must complete PS Form 1360, *Information Systems Security Incident Report*, to ensure appropriate security management notification of the status and disposition of the information resource.

3-5.8 Disposal and Destruction of Information and Media

3-5.8.1 Electronic Hardware and Media

To prevent inadvertent disclosure of sensitive-enhanced and sensitive information, all electronic hardware and media must, prior to being disposed of, undergo data eradication according to approved Postal Service procedures. Unacceptable practices of erasure include a high-level file erase or high-level formatting that only removes the address location of the file. Acceptable methods of complete erasure include the following:

a. Zero-bit formatting.

b. Degaussing.

c. Physical destruction.

The results from zero-bit formatting and degaussing must be periodically tested to verify complete erasure.

Disposal contractors must have appropriate personnel clearances, physical security of the facility, and procedures to store and handle the equipment and media (that may contain sensitive-enhanced or sensitive information) before and during disposal.

3-5.8.2 Data Residue

As resources are allocated to data objects or released from those data objects (i.e., object reuse), information resources must have the capability to ensure that no accessible data is exposed to unauthorized users. Information resources must:

a. Have the capability to overwrite memory and storage that renders the information unrecoverable to prevent disclosure of sensitive-enhanced and sensitive information.

b. Restrict the capability to overwrite memory and storage to an authorized user.

c. Ensure that any previous information content of a resource is made unavailable upon the re-allocation of the resource for usage.

3-5.8.3 Nonelectronic Information

Nonelectronic information designated as sensitive-enhanced or sensitive must be destroyed by shredding, pulping, or burning when no longer needed if the information is not subject to a legal hold and the retention period has expired.

3-6 Protection of Non-Postal Service Information

3-6.1 Third-Party Information

Any information that does not belong to the Postal Service must be protected in accordance with legal requirements or contractual agreements with a third party except that when such requirements do not meet security standards for comparable Postal Service information, the Postal Service must meet or exceed its own standards.

3-6.2 National Security Classified Information

Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

4 Security Risk Management

4-1 Policy

Risk assessments are required for all information resources, whether developed and operated in house or by business partners to ensure cost-effective protection of information, applications, information resources, and the continuity of business operations. Site security reviews are also required for all facilities that house sensitive-enhanced, sensitive, or critical information resources, regardless of where they are located. Based on the results of risk assessments and site security reviews, managers must develop (or acquire) and implement security measures to handle unexpected events, avoid unacceptable losses, and minimize the effect of emergencies on business operations. Chapter 4 addresses the following:

a. Types of risk management.
b. Information resource risk management.
c. Independent risk management.
d. Site risk management.

4-2 Types of Risk Management

The Postal Service implements the following three types of risk management:

a. Information resource risk management.
b. Independent risk management.
c. Site risk management.

4-3 Information Resource Risk Management

A risk assessment must be completed for all information resources. The risk assessment must address the following areas:

a. Identify the assets at risk and their value to the organization.
b. Identify the threats.
c. Identify the weaknesses and vulnerabilities.
d. Evaluate threats and vulnerabilities to determine the risks that threaten loss of value.
e. Identify possible safeguards (e.g., controls and countermeasures).

f. Analyze the costs and benefits of the safeguards in reducing the risks.

g. Complete the information resource risk assessment report.

The risk assessment must be completed in conjunction with system development. Additional risks may be identified in each of the life-cycle phases as development progresses through requirements definition, design, coding, testing, and production. The risks must be re-assessed and the risk assessment report updated as follows:

a. At least every 3 years following deployment of a sensitive-enhanced, sensitive, or critical information resource as part of the recertification process unless earlier re-assessment is warranted.

b. Every year for a payment card industry information resource.

c. After a significant audit finding.

d. Whenever the information resource experiences significant enhancement or modification, including changes to the infrastructure, operating system, or hardware platform.

e. After an information security incident that violates an explicit or implied security policy and compromises the integrity, availability, or confidentiality of an information resource.

Risks categorized as high must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures. The risk mitigation process consists of the following:

a. Selecting the appropriate safeguards (or countermeasures) that will reduce exposure to the risk.

b. Assigning a priority ranking to the implementation of the safeguards.

c. Assigning financial and technical responsibility for implementing the safeguards.

d. Implementing and documenting the safeguards.

e. Maintaining the continued effectiveness of the mitigation strategy by periodically reassessing the threats, vulnerabilities, effectiveness of the safeguards, and the residual risk.

If the level of residual risk is not acceptable, then further safeguards and security controls should be implemented to reduce exposure to acceptable levels. The vice president of the functional business area and the vice president, Information Technology Operations are jointly responsible for acknowledging and accepting, in writing, the residual risks inherent with using that information resource or initiating steps to further mitigate the residual risk.

All information resource risk management documentation must be treated as “restricted information” delivered to and retained by the executive sponsor and a copy sent to the Corporate Information Security Office.

4-4 Independent Risk Management

An independent information risk assessment may be required during the business impact assessment process. Independent risk assessments are conducted by organizations that are separate and distinct from those responsible for the development and operation of the information resources. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process,* for the criteria for conducting an independent risk assessment.)

4-5 Site Risk Management

A site security review must be performed for each site hosting sensitive-enhanced, sensitive, or critical information resources and may be required for business partner and vendor sites requesting connectivity to the Postal Service intranet to:

a. Identify the location of the facility and structure-specific strengths and weaknesses.

b. Identify the sensitive-enhanced, sensitive, and critical information resources hosted by that facility.

c. Identify the threat events that could occur, including physical threats (e.g., power failure, fire, building collapse, water damage from plumbing failure and roof leak); environmental threats (e.g., earthquake, flooding, tornadoes, lightning, and sink hole); and human threats (e.g., union lockouts, riot, disgruntled employee or customer, and armed theft).

d. Evaluate threats and vulnerabilities to determine the frequency and amount of harm that could possibly occur as a result of a physical, environmental, or human event.

e. Identify possible additional administrative, technical, and physical security safeguards.

f. Analyze the costs and benefits of the safeguards in reducing the risks.

A site security review is conducted at the following times:

a. Before a new site becomes operational.

b. After significant changes at the site, including significant changes in information resources located there.

c. At least every 3 years, unless an earlier site security review is warranted.

Risks categorized as high must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures. The risk mitigation process consists of the following:

a. Selecting the appropriate safeguards (or countermeasures) that will reduce exposure to the risk.

b. Assigning a priority ranking to the implementation of the safeguards.

c. Assigning financial and technical responsibility for implementing the safeguards.

d. Implementing and documenting the safeguards.

e. Maintaining the continued effectiveness of the mitigation strategy by periodically reassessing the threats, vulnerabilities, effectiveness of the safeguards, and the residual risk.

If the level of residual risk is not acceptable, then further safeguards and security controls should be implemented to reduce exposure to acceptable levels. The installation head is responsible for acknowledging and accepting the residual site risk.

All site risk management documentation must be treated as “restricted information” and delivered to and retained by the Inspection Service and the appropriate installation head.

5 Acceptable Use

5-1 Policy

Postal Service information resources must be used in an approved, ethical, and lawful manner to avoid loss or damage to Postal Service operations, image, or financial interests and are used to comply with official policies and procedures on acceptable use. Personnel must contact the manager, Corporate Information Security Office, prior to engaging in any activities not exactly explicitly covered by the following policies:

a. Personal use of government office equipment including information technology.

b. Electronic mail and messaging.

c. Internet.

d. Prohibited uses of information resources.

e. Protection of privacy.

5-2 Personal Use of Government Office Equipment Including Information Technology

Management at each Postal Service facility may permit employees to make limited personal use of Postal Service office equipment, including information technology, provided such use does not reduce or otherwise adversely affect the employee's productivity during work hours, does not interfere with the mission or operations of the Postal Service, and does not violate the Standards of Ethical Conduct.

The office equipment governed by this policy includes, but is not limited to, personal computers; personal digital assistants (including Blackberries); peripherals, such as printers and modems; computer software (including Web browsers); telephones; cell phones; facsimile machines; photocopiers; scanners; label writers; consumable office products; office supplies; library resources; Internet connectivity; and e-mail. Use of Postal Service information resources constitutes permission to monitor that use.

Limited personal use of Postal Service office equipment, including information technology, means occasional use that meets the following criteria:

a. Is of limited duration, length, or size, and does not interfere with employees' official duties or the transaction of official Postal Service business.

b. Results in only minimal, if any, additional expense to the Postal Service or minimal wear and tear on Postal Service office equipment; uses a small amount of data storage; has only a small-to-moderate transmission impact; or requires only small amounts of consumable office products (e.g., ink, paper, toner, and computer memory).

Some examples of limited personal use are:

a. Making a few photocopies.

b. Make occasional, brief telephone calls that result in little or no cost.

c. Sending an occasional facsimile of a few pages.

d. Sending a brief e-mail message.

e. Doing a brief Internet search.

Limited personal use of Postal Service office equipment, including information technology, must not:

a. Reduce employee productivity or interfere with official Postal Service business (e.g., congest, delay, or disrupt any Postal Service system or equipment).

b. Be for the purpose of maintaining or promoting a personal or private business.

c. Be for the purpose of posting unauthorized commercial or advertising materials.

d. Be for any illegal purpose, including, but not limited to, gaining unauthorized access to other systems; disseminating any discriminatory or hate-based materials or speech; or reproducing or distributing copyrighted, trademarked, proprietary, or export-controlled data or software.

e. Be in relation to sexually explicit or sexually oriented materials.

f. Refer or relate to illegal gambling, illegal weapons, and/or terrorist activities.

g. Be for the purpose of fundraising, endorsing any product or service, lobbying, or participating in any prohibited partisan political activity.

h. Be for the purpose of using applications and/or software that have not been approved by the Postal Service and that occupy or impact official computer or network processing time.

i. Result in the disclosure of any Postal Service information that is not otherwise public.

Use of Postal Service office equipment in violation or excess of the limited personal use permitted by this policy may result in limitations on future use, administrative action, criminal penalty, and personal financial liability.

For advice on how to avoid violating this policy and the corresponding misuse of government property prohibitions in the Standards of Ethical Conduct, please call the Postal Service's Ethics Helpline at 202-268-6346 or send an e-mail to *ethics.help@usps.gov.*

5-3 Electronic Mail and Messaging

Access to the Postal Service electronic mail (e-mail) system is provided to personnel whose duties require e-mail to conduct Postal Service business. If you do not comply with Postal Service e-mail policies your e-mail account may be suspended and you will have to request your manager apply to the vice president, Information Technology Operations for reinstatement of the lost privileges. Only Postal Service-provided e-mail services may be accessed from Postal Service information resources. Since e-mail may be monitored, anyone using Postal Service resources to transmit or receive e-mail should not expect privacy.

Sensitive-enhanced and sensitive information must be only sent to authorized personnel with a need to know.

Although occasional and incidental personal e-mail use is permitted, personal messages while they remain in the system will be considered to be in the possession and control of the Postal Service.

5-3.1 Prohibited Use

Do not use Postal Service information resources to check personal e-mail accounts (e.g., Hotmail, Yahoo, Excite, MSN). Other prohibited activities when using Postal Service e-mail include, but are not limited to, sending or arranging to receive the following:

a. Information that violates state or federal laws or Postal Service regulations.

b. Information designated as sensitive-enhanced or sensitive information unless encrypted according to Postal Service standards.

c. Unsolicited commercial announcements or advertising material.

d. Any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the Postal Service, the recipient, the sender, or any other person.

e. Pornographic, sexually explicit, or sexually oriented material.

f. Racist, hate-based, or offensive material.

g. Viruses or malicious code.

h. Chain letters, unauthorized mass mailings, or any unauthorized request that asks the recipient to forward the message to other people.

5-3.2 Encryption

Encrypting e-mail or messages must comply with the following:

a. Encryption software and methods must be approved by the Enterprise Architecture Committee.

b. Encryption solutions must either support key recovery or keys must be registered with authorized personnel.

c. Recovery keys or other similar files for all encrypted e-mail must be placed in a directory or file system that can be accessed by management prior to encrypting e-mail.

d. Recovery keys or other devices needed to decrypt e-mail must be provided when requested by authorized Postal Service management, the Postal Inspection Service or the Office of Inspector General.

e. Keys may not be escrowed in customer product offerings unless specifically requested in writing by the customer and approved by the executive sponsor.

5-4 Internet: Access and Prohibited Activities

Access to the Internet is available to employees, contractors, subcontractors, and business partners whose duties require access to conduct Postal Service business. Since Internet activities may be monitored, all personnel accessing the Internet will have no expectation of privacy.

Prohibited activities when using the Internet include, but are not limited to, the following:

a. Browsing explicit pornographic or hate-based Web sites, hacker or cracker sites, or other sites that the Postal Service has determined to be off limits.

b. Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material the Postal Service has determined to be off limits.

c. Posting or sending sensitive-enhanced or sensitive information outside of the Postal Service without management authorization.

d. Hacking or other unauthorized use of services available on the Internet.

e. Posting unauthorized commercial announcements or advertising material.

f. Promoting or maintaining a personal or private business.

g. Receiving news feeds, push data updates, or continuous data streams unless the material is required for Postal Service business.

h. Using non-Postal Service approved applications or software that occupy or use workstation idle cycles or network processing time (e.g., processing in conjunction with screen savers).

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 or copying of electronic files not related to your normal business activities without management approval.

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 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 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 the Postal Service, its personnel, business partners, or customers.

n. Using someone else's logon ID and password.

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 personal information resources to the Postal Service intranet (Blue).

q. Using 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, or other Postal Service areas unless approved by area or headquarters vice president

or designee for business purposes. (See Management Instruction AS-882-2007-6, *Postal Service Use of Retail and Cell-Phone Cameras,* on the use of handheld and cell phone cameras.)

5-6 Protection of Privacy

Information resources must protect the privacy-related data of customers and all personnel 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.* Postal Service privacy policy for customers is posted on *www.usps.com*.

6 Personnel Security

6-1 Policy

The Postal Service identifies sensitive positions and ensures that individuals assigned to those positions have the appropriate level of clearance to minimize risk to Postal Service information resources.

Personnel are held accountable for carrying out their information security responsibilities. Managers must ensure personnel receive appropriate information security training and protect Postal Service resources when personnel depart under involuntary or adverse conditions.

Policies addressed in this chapter are the following:

- Employee accountability.
- Sensitive positions.
- Background investigations and clearances.
- Information security awareness and training.
- Departing personnel.

6-2 Employee Accountability

6-2.1 Separation of Duties and Responsibilities

Personnel must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud, or collusion.

6-2.2 Job Descriptions

The Postal Service defines and documents the information security requirements for each position.

6-2.3 Performance Appraisals

The Postal Service evaluates the execution of information security responsibilities and the compliance with information security policies and procedures in personnel performance appraisals.

6-2.4 Condition of Continued Employment

The Postal Service includes the execution of information security responsibilities and the compliance with information security policies and procedures as a condition of continued employment for all personnel.

6-2.5 Sanctions

All personnel are held accountable for carrying out their information security responsibilities. Violators of Postal Service information security policies are subject to progressive sanctions commensurate with the severity and frequency of the infraction, including disciplinary action, removal, or criminal prosecution.

6-3 Sensitive Positions

Managers at all levels are responsible for identifying sensitive positions within their organizations and then requesting the chief postal inspector to designate the positions as sensitive.

Sensitive positions, as defined in the *Administrative Support Manual* (ASM) 27, Security, include those in which personnel could, in the normal performance of their duties, cause material adverse effect to Postal Service information resources. Such duties include, but are not limited to, the following:

a. Making changes in the operating system, configuration parameters, system controls, and audit trails.

b. Modifying security authorizations.

c. Making revisions to sensitive programs and data that could be undetected.

6-4 Background Investigations and Clearances

6-4.1 General Requirements

Personnel must have appropriate background investigations and personnel clearances as determined by the Postal Inspection Service before accessing Postal Service information resources (see ASM 272, Personnel Security Clearances). For personnel without clearances, access is restricted to temporary information services (see 9-3.2.2, Temporary Information Services).

Appropriate background investigations must be conducted and personnel clearances obtained for personnel who access sensitive-enhanced, sensitive, or critical information resources, require unescorted access to controlled areas, or perform the duties of a sensitive position.

6-4.2 Access Privileges

6-4.2.1 Logon IDs

Managers must use eAccess to request access authorization for individuals who do not have the appropriate clearance and are responsible for the access activities of those individuals.

6-4.2.2 Information Resources Processing Sensitive-Enhanced or Sensitive Information

All personnel whose duties require access to Postal Service information resources processing sensitive-enhanced or sensitive information (see 3-2, Information Designation and Categorization) must have an appropriate clearance as determined by the Inspection Service before they obtain access (see ASM 272, Personnel Security Clearances).

6-4.2.3 Controlled Areas

All personnel, whose duties require unescorted access to controlled areas, whether located at a Postal or non-Postal Service facility, must have an appropriate clearance as determined by the Inspection Service before being granted unescorted access privileges.

6-4.3 Foreign Nationals

In certain situations, personnel may be permanent resident aliens and citizens of foreign countries and still provide services to the Postal Service, with prior approval of the responsible executive (see ASM 272.322, Citizenship). Except for citizenship, foreign nationals must meet the same clearance requirements as all other personnel. The Postal Service executive who approves access to information resources by foreign nationals (including contractors) is responsible for all actions initiated by the foreign national.

6-5 Information Security Awareness and Training

6-5.1 General Security Awareness

All managers must continually strive to incorporate information security into training courses, training videos, service talks, internal newsletters, posters, case studies, and other tools and visual aids to increase information security awareness among all personnel. The training should explain how anyone failing to comply with security policies and procedures will be disciplined.

6-5.2 Documenting and Monitoring Individual Information Security Training

Individual information security training activities must be documented and monitored to ensure all personnel attend their initial, annual, and operational training (as required) before given access to sensitive-enhanced, sensitive, or critical information.

6-5.3 Training Requirements

Exhibit 6-5.3
Training Requirements

Training Type	Requirement(s)
Annual Training	All personnel must participate at least annually in ongoing information security awareness and training activities as a component of Voice of Employee requirements.
Information Resource Operational Security Training	All personnel must be trained to handle security breaches and incidents. For information resources processing sensitive-enhanced, sensitive, or critical information appropriate operational security training must be developed and conducted. The training should explain how to protect information throughout its life cycle and report incidents.
New Personnel Training	All new personnel must receive information security training and be issued a copy of Handbook AS-805-C, *Information Security for General Users*.

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 nonadverse circumstances, the individual's manager, supervisor, or contracting officer must ensure the following:

a. All accountable items, including keys, access cards, two-factor credentials, laptop computers, and other computer-related equipment are returned.

b. The individual's computer logon ID and building access authorizations are terminated coincident with the employee's or contractor's effective date of departure, unless needed in the new assignment.

c. 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 contracting officer of an individual being terminated under adverse circumstances must:

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 logon 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. Destroy or transfer sensitive-enhanced or sensitive information to another custodian.

f. Notify the Postal Inspection Service.

6-6.3 Systems or Database Administrator Departure

Routine separation or adverse termination of a systems administrator or a database administrator requires taking extra care and precautions. Upon departure, remove the privileged access as quickly as possible to maintain the security and integrity of the specific information resources to which the administrator had access. After departure, monitor the affected information resources for improper use or access. Specifically, the manager, supervisor, or contracting officer of the departing systems or database administrator must:

a. Follow the requirements documented above for routine separation or for adverse termination as applicable.

b. Reconfigure access lists to remove the departed administrator's accounts.

c. Disable or change the password or login requirements to all shared devices and applications.

d. Disable or change passwords to all shared service and privileged accounts.

e. Disallow physical access to buildings, systems, and information associated with the departed administrator's former access.

f. Monitor all privileged accounts for usage and access to the systems, applications, and databases formerly under the administrator's control to ensure all access has been removed.

g. Review records for Postal Service information approved for removal offsite and make appropriate efforts to recover information and/or equipment as applicable. Notify the manager, Corporate Information Security Office, of any information identified as removed but not recovered.

This page intentionally left blank

7 Physical and Environmental Security

7-1 Policy

The Postal Service protects its information resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorized personnel.

Where possible, all information resources (including portable information resources) must reside in a protected environment. Physical and administrative security controls must be implemented at each facility to protect against unauthorized personnel access and to protect the physical integrity of Postal Service information resources located at the facility. Such physical and administrative security controls include the following:

a. Physical access controls.

b. Physical protection of information resources.

c. Environmental security.

d. Facility continuity planning.

e. Facility contracts.

7-2 Physical Access Controls

7-2.1 Access to Controlled Areas

Access to controlled areas must be restricted as follows:

a. Access to controlled areas is restricted to personnel whose duties require access to such facilities and who possess appropriate security clearances.

b. Access to controlled areas must be controlled by electromechanical means. Personnel authorized access to the controlled areas must always use their access control identification badge or device to gain entrance to the controlled area. Tailgating is prohibited and personnel are responsible for immediately reporting any instance of tailgating.

c. A record of physical access, both authorized individuals and visitors, must be maintained. Automated mechanisms should be employed where feasible to facilitate the maintenance and review of access records.

d. Personnel without an authorized Postal Service identification badge or device must sign a visitor log and be escorted by authorized personnel while in the controlled area.

e. Visitor logs must include at a minimum: name and organization of the person visiting, form of identification used for authentication, date of visit, time of entry and departure, purpose of visit, and name of person and organization visited. Visitor logs must be reviewed periodically and security violations and suspicious activities must be investigated and remedial actions taken.

7-2.2 Establishment of Controlled Areas

Controlled areas must be established within the facility wherever more stringent restrictions on physical access and more tightly controlled physical and environmental security are required to fully protect information resources. Typical controlled areas may include the following:

a. Computer rooms.

b. Telecommunications rooms.

c. Wiring closets.

d. Computer operations areas.

e. Media and documentation storage areas.

f. Operating system software support areas.

g. Special authorization terminal areas.

h. Security officers' controlled areas.

i. Other designated areas, whether located at a Postal Service or non-Postal Service facility.

7-2.3 Types of Information Resources Stored in Controlled Areas

Information resources processing sensitive-enhanced, sensitive, or critical information must be located in a controlled area.

7-2.4 Establishment of Access Control Lists

Each controlled area must establish an access control list of people who are authorized access. Access control lists must be updated when new personnel are assigned to the controlled area or when someone leaves. Access control lists must also be reviewed, updated periodically, and posted within the controlled area. Data center access must be reviewed by the designated Information Technology manager on a quarterly basis.

Personnel not on the access control list must sign a visitor log and be escorted by authorized personnel while in the controlled area.

7-2.5 Training for Controlled Areas

Personnel with access to controlled areas must be trained in their responsibilities regarding controlled areas.

7-2.6 Installation of Physical Access Control Devices

Physical access control devices using biometrics, smart cards, tokens, mantraps, or lockable cabinets may be installed to supplement traditional facility locks and keys to limit access. Additionally, the Inspection Service and Facility Management may require physical access to be monitored by surveillance equipment and real time intrusion detection and alarm systems (e.g., CCTV, motion detectors, and other audio or silent alarms) to detect and respond to incidents [see the *Administrative Support Manual* (ASM) 273, Facility Security, and Handbook RE-5, *Building and Site Security Management].*

Based on the risks associated with the information resource, additional physical access security mechanisms (e.g., locked cabinet or desk, portable device cable lock, and biometric workstation lock) must be implemented for information resources processing sensitive-enhanced, sensitive, or critical information.

Security personnel are notified immediately of physical security events and follow-up action is taken and documented.

7-2.7 Implementation of Identification Badges

Identification badges must adhere to the following criteria:

a. Persons authorized access to controlled areas must be identified by a picture badge conspicuously displayed on their person.

b. Persons using a badge not issued to them or making any attempt to alter a badge will be subject to disciplinary action.

c. Employees must report lost or stolen badges immediately to the issuer of the badge.

d. Security access systems that limit access to controlled areas where persons have reported lost or stolen badges must immediately cancel the associated access privileges until the lost or stolen badge is recovered and returned to the issuer.

e. Temporary badges must be controlled and issued by the manager of the organization or their designee to authorized personnel who arrive without their assigned badges during normal duty hours.

f. The organization manager or designee must make an unannounced verification of badges at least annually to ensure authenticity and to correct any badge discrepancies.

7-3 Physical Protection of Information Resources

Information resources must be protected against damage, unauthorized access, and theft, both in the Postal Service environment and when removed from this secure environment.

Note: Sensitive-enhanced and sensitive information stored on removable devices or media must be encrypted and stored in a controlled area or in a locked cabinet. Sensitive-enhanced and sensitive

information that is stored off Postal Service premises must also be encrypted and stored in a controlled area or in a locked cabinet.

7-3.1 Network Equipment, Network Servers, and Mainframes

Network equipment, network servers, and mainframes must be protected against damage, unauthorized access, and theft and, where possible, housed in separate rooms that can be accessed only by authorized personnel.

Additional protection measures to control physical access to information distribution and transmission include locked wiring closets, disconnected or locked spare jacks, and protection of cabling with conduit or cable trays.

7-3.2 Postal Service Workstations and Portable Devices

Postal Service workstations and portable information resources must be protected at all times in use, storage, and in transit against damage, unauthorized access, and theft.

7-3.3 Non-Postal Service Portable Electronic Devices

To protect Postal Service information from disclosure or compromise, non-Postal Service portable devices [e.g., laptops, notebooks, personal digital assistants ([PDAs), handheld computers, or storage media including universal serial bus (USB) port devices or thumb drives] should not be used on Postal Service facilities without approval from the user's vice president or his or her designee. Under no circumstances will such devices connect to the Postal Service intranet (Blue) or store Postal Service information.

Visitors to Postal Service facilities are required to present non-Postal Service portable devices to the installation head or his or her designee upon entry to the facility. The installation head or his or her designee determines if such devices must be surrendered for the duration of the visit. Under no circumstances will such devices connect to the Postal Service intranet or store Postal Service information.

7-3.4 Sensitive-Enhanced, Sensitive, and Critical Media

Sensitive-enhanced, sensitive, and critical media, whether electronic or nonelectronic, must be protected against physical loss or damage, whether on Postal Service premises or not. Physical and administrative controls must be implemented to ensure that only authorized personnel can access sensitive-enhanced, sensitive, and critical information. Personnel who have custody of sensitive-enhanced, sensitive, and critical media are responsible for their safekeeping (see 3-5, Protection of Postal Service Information and Media).

7-4 Environmental Security

Environmental security controls must be implemented at the facility, room, and information resource level to protect servers, mainframes, and critical information resources as described below:

a. Protection against lightning, wind, and building collapse must be implemented.

b. Protection against water damage from water supply lines, sewer systems, and roof leaks must be implemented (e.g., plastic sheets are available and master shutoff valves are accessible, working properly, known to operations personnel, and automatic where feasible).

c. Additional temperature and humidity safeguards must be implemented to monitor and maintain acceptable levels.

d. Protection against flooding, earthquakes, or other natural disasters must be implemented (e.g., drains are installed below the computer room floor).

e. Additional fire safeguards:

- Fire detection and suppression equipment (e.g., smoke and heat detectors, handheld fire extinguishers, fixed fire hoses, and sprinkler systems) must be implemented.
- Fire detection and suppression equipment must automatically notify the organization and emergency responders.

f. Additional power (electricity) safeguards:

- A short-term alternate power supply must be implemented to ensure proper shutdown in the event of a power interruption.
- A long-term alternate power supply must be implemented to maintain minimal operational capability in the event of a power outage.

g. Automatic emergency lighting systems must be implemented to illuminate emergency exits and evacuation routes in the event of a power outage or disruption.

h. Surge protection must be implemented for all information resources.

i. Redundant power feeds and redundant communications paths must be implemented for critical information technology sites.

For areas containing concentrated information resources, Facility Management may require the capability to shut off power to information resources that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to potential flooding) without endangering personnel by requiring them to approach the equipment. See ASM 273, Facility Security, and Handbook RE-5, *Building and Site Security Management*, for the requirements for remote power shutoffs.

7-5 Facility Continuity Planning

Physical security requirements must be included in facility continuity planning to ensure the appropriate protection of information resources following a catastrophic event.

7-6 Facility Contracts

Information, environmental, and physical security requirements must be included in contracts involving facilities to ensure the appropriate protection of information resources.

8 Development and Operations Security

8-1 Policy

Information resources must be developed under the technical solutions life cycle (TSLC) or other approved system development life cycle methodology. Information security must be an integral part of the system development life cycle whether development is done in house, acquired, or outsourced. Postal Service information must also be appropriately protected during operation. Security activities must be performed to maintain a secure environment and to comply with Postal Service policies and legal requirements.

The Postal Service certification and accreditation (C&A) process defines a formal review process that ensures adequate security is incorporated during each phase of the project life cycle. The C&A process is required for each information resource (i.e., application or infrastructure component).

Chapter 8 addresses the following topics:

a. Development security.

b. Operations security.

c. Certification and accreditation.

8-2 Development Security

8-2.1 Life Cycle Approach

Security must be addressed throughout the information resource life cycle process, from requirements, design, build, system integration testing (SIT), customer acceptance testing (CAT), release (and production) and retirement. All development, acquisition, or integration projects for information resources, whether performed in house or by a business partner, must follow the TSLC process or other approved systems development life cycle methodology.

8-2.2 Risk Management

A risk-based approach must be applied to information security that uses limited resources wisely to protect an information resource in a cost-effective

manner throughout its life cycle. The security controls applied to information resources must be commensurate with the magnitude of harm that would result from loss, misuse, unavailability, unauthorized access, or unauthorized modification of the information resources (see 4-3, Information Resource Risk Management).

8-2.3 Quality Assurance

Information resource development must include quality assurance (QA) and security-specific testing to ensure that security controls have been implemented and are functioning correctly. Transactions failing edit and validation routines must be subject to appropriate follow-up until errors are remediated. Information processing failures discovered as the result of remediation must be used for root cause analysis and to adjust procedures and automated controls to improve quality.

8-2.4 Configuration and Change Management

All information resources, whether developed in house, outsourced, or acquired must be developed under standard configuration and change management procedures to reduce the risk introduced by undocumented and untested changes in accordance with the Postal Service change management policy/procedure. Postal Service information resources must not be developed or deployed unless a change and configuration management process is in place.

Configuration and change control involve the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. Appropriate organizational officials approve information system changes in accordance with this process. Emergency changes are also included in the configuration and change control process.

8-2.4.1 Configuration Component Inventory

To effectively manage information resources, the information system components must be inventoried and the initial or baseline configuration of the information resources must be documented prior to deployment. The inventory of information system components must include manufacturer, type, serial number, version number, information system/component owner, and location (i.e., physical location and logical position within the information system architecture). The inventory must also designate those information system components required to implement and/or conduct contingency planning operations.

Configurations of information resources must be periodically reviewed to ensure the documented configuration matches the actual current components.

8-2.4.2 Configuration Hardening Standards

Hardware and system software must be hardened to Postal Service information security requirements. Configuration hardening standards must be used to maintain a high level of information security, enable cost-effective and timely maintenance and repair, and protect Postal Service information

resources against unexpected vulnerabilities. See the manager, Corporate Information Security Office (CISO) Information Security Services (ISS), to request access to a specific Postal Service configuration hardening standard.

8-2.4.3 Change and Version Control

Changes to information resources and configurations must be managed to ensure that Postal Service information resources are not inadvertently exposed to unnecessary risks and vulnerabilities and that only qualified and authorized individuals initiate changes, upgrades, and modifications. Individual access privileges must be approved by appropriate management officials.

All changes must be appropriately approved and documented. Application code changes are managed using version control software. Change control records must be maintained to support and document system software maintenance, software and hardware upgrades, and any local system modifications.

8-2.4.4 Patch Management

An effective patch management process must be implemented to investigate, prioritize, test, track, control the deployment and maintenance of software releases, and resolve known security vulnerabilities. The patch management process must address all information resources installed in the Postal Service computing environment. Security patches must be installed in a timely manner following established evaluation and implementation processes. Software security patches must be evaluated on a regular basis based on platform and implemented if appropriate. Evaluation periods include: semi-annually for UNIX, DB2, IDMS and COTS; quarterly for Oracle; and monthly for Windows. Software patch evaluations must be properly documented and retained in the appropriate repository. Personnel involved in the patch management process must be trained to ensure a viable vulnerability mediation process.

Patch management involves acquiring, testing, and installing multiple patches (code changes) to software systems, including operating system software, supporting software and packages, firmware, and application software. Patch management tasks include the following:

a. Maintaining current knowledge of available patches.
b. Deciding what patches are appropriate for particular information resources.
c. Prioritizing the patches to be installed.
d. Testing patches in a nonproduction environment first in order to check for unwanted or unforeseen side effects.
e. Developing a back-out plan which includes backing up the systems about to be patched to be sure that it is possible to return to a working configuration.
f. Ensuring that patches are installed properly.
g. Testing information resources after installation.

h. Documenting all associated procedures, such as specific configurations required.

Patch management is critical to ensure the integrity and reliability of information resources. Patch management should be capable of:

a. Highly granular patch update and installation administration (i.e., treating patches and mainframes, servers, desktops, and laptops separately).

b. Tracking machines, and updating and enforcing patches centrally.

c. Verifying successful deployment on each machine.

d. Deploying client settings, service packs, patches, hot fixes, and similar items network-wide in a timely manner in order to address immediate threats.

e. Initiating from a central management console.

f. Providing scheduling, desktop management, and standardization tools to reduce the costs associated with distribution and management.

g. Providing ongoing deployment for both new and legacy systems in mixed hardware and operating system environments.

h. Automating the repetitive activity associated with rolling out patches.

i. Analyzing the operating system and applications to identify possible security holes.

j. Scanning the entire network (IP address by IP address) and providing information such as service pack level of the machine, missing security patches, key registry entries, weak passwords, users and groups, and more.

k. Analyzing scan results using filters and reports to proactively secure information resources (e.g., installing service packs and hotfixes).

8-2.4.5 Security Testing of the Configuration

After the information system is changed, the security controls must be checked to ensure the security features are still functioning properly. Periodically (at a minimum annually), the security controls must be tested to ensure the information security controls are functioning as designed and documented.

Significant changes (as defined in 8-9.7.9, Re-initiate C&A) will cause the re-initiation of the C&A process.

8-2.5 Separation of Duties

An individual or organization must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for accidental or malicious wrongdoing, fraud, or collusion. When it is not possible for duties to be assigned to separate individuals, the roles and functions performed must be clearly defined, associated activities logged, security-related functions audited, and compensating controls identified and implemented. The CISO reserves the right to validate the effectiveness of the compensating controls.

8-3 Operations Security

8-3.1 Postal Service Environments

The TSLC defines the following four logical environments as follows:

a. Development (DEV).

b. SIT.

c. CAT.

d. Production (PROD).

National systems/applications must be engineered with a minimum of three separate environments. The three separate environments must have at least four logical environments that are DEV, SIT, CAT and PROD. In a three-separate environment approach, the acceptable groupings of these four logical environments in the three separate environments are DEV/SIT, CAT, PROD or DEV, SIT/CAT, PROD. In the latter grouping, the SIT environment must be cleared before it becomes the CAT environment.

8-3.2 Environment Restrictions

Restrictions are defined for the following environments:

a. DEV.

b. SIT.

c. CAT.

d. PROD.

8-3.2.1 Development Environment

Developers get full access (e.g., read, write, execute, allocate, and delete) in this environment to application software. Restrictions for the development environment include the following:

a. Developers are restricted to read and execute privileges for database and operating system software.

b. Test data containing personally identifiable information (PII) and payment card industry (PCI) cardholder data must be de-identified.

c. No access to production systems is allowed from this environment.

d. Development environment is an isolated infrastructure (DEVSUB) or enclaved.

8-3.2.2 SIT Environment

Developers are restricted to read and execute privileges to application, database, and operating system software in the SIT environment. Code is migrated from the SIT environment back to the development environment to apply updates/fixes. Restrictions for the SIT environment include the following:

a. Developers may have access to the SIT environment with documented management approval.

b. Systems moved to the SIT environment are documented and managed by a version control library system.

c. Personally identifiable information (PII) or cardholder data must be de-identified prior to use in the SIT environment; any exception to the de-identification requirement must be approved by the chief information officer (CIO), chief privacy officer (CPO), and the executive sponsor manager. If the usage of PII or cardholder data that is not de-identified is approved for use in the SIT environment, the SIT environment must implement the same controls and security requirements as production.

8-3.2.3 CAT Environment

Access is restricted to production operations personnel, executive sponsorship, and developers with proper authorization. The CAT environment must implement the same controls and security requirements as production. Restrictions for the CAT environment include the following:

a. Developers may have access to the CAT environment with documented management approval.

b. Systems moved to the CAT environment are documented and managed by a version control library system.

c. PII or PCI cardholder data must be de-identified prior to use in the CAT environment; any exceptions to the de-identification requirement must be approved by the CIO, CPO, and the executive sponsor. If cardholder data that is not de-identified is approved for use in the CAT environment, the cardholder data must be encrypted.

8-3.2.4 Production Environment

Restrictions for the production environment include:

a. Developers must not have ongoing or privileged access to application, database, and operating system software in this environment.

b. Developer access to production systems must be authorized by the executive sponsor, CIO, and CPO via eAccess or PS Form 1357, *Request for Computer Access.*

c. Access to the production system, if approved, must be managed, documented, and restricted to read.

d. The developer account must be temporary and disabled/removed upon completion of the task.

e. Developer access must be logged while the account is active.

f. The CISO must be informed of the access.

g. Production data must not be copied by the developer.

h. Extreme care must be exercised when accessing PII and cardholder information. If not necessary for the task, PII and cardholder data must be masked from view or de-identified. De-identifying production data is the process of systematically masking or transforming PII and cardholder data elements so they can no longer be used identify an individual or cardholder data.

8-3.2.5 Other Environments

The restrictions are the same as for the development environment.

8-3.3 Testing Restrictions

All information resources must comply with the testing restriction policies below. These restrictions apply to modules and to applications. Separate approvals are required for each module.

The SIT and CAT environments must be representative of the operating landscape, including likely workload stress, operating system, application software, database management systems, and network/computing infrastructure found in the production environment. As the production environment changes, the test environment must also change to stay in synchronization.

The testing must only be conducted within the CAT environment by a test group independent from the development team using clearly defined test instructions (scripts) and interactive testing that adequately address the testing requirements and success criteria defined in the test plan. Errors found during testing must be logged, classified (e.g., minor, significant, and mission critical), and communicated to key stakeholders.

8-3.3.1 Development and Testing in the Production Environment

Development and testing of hardware and software must not be performed in the production environment.

8-3.3.2 Testing With Nonsensitive Production Data

Prior approval in writing is required from the executive sponsor and CIO or designee if nonsensitive production data is to be used in a test environment, regardless of where the testing is conducted. Such approved production data files must be identified as “copies” to prevent them from being re-entered into the production environment.

8-3.3.3 Testing with Sensitive-Enhanced and Sensitive Production Data

Prior approval in writing is required from the CPO, executive sponsor, and CIO or designee if sensitive-enhanced and sensitive information is to be used in a test environment, regardless of where the testing is conducted. Approved data files must identified as “copies” to prevent them from being re-entered into the production environment.

Prior to usage of production data in a test environment, the test environment must be hardened to production standards.

PII or cardholder data must not be placed in the test environment without being de-identified. The masked/transformed data elements must then be propagated across related tables within the database to preserve the integrity of data relationships, maintain the referential integrity of the test data, and ensure the validity of test results.

8-3.3.4 Testing at Non-Postal Service Facilities with Production Data

Additional approval in writing is required from the manager, CISO, if production data is to be used in a test environment outside of Postal Service facilities. Such approved files must be identified as “copies” to prevent them from being re-entered into the production environment.

8-4 Certification and Accreditation

C&A is a formal security analysis and management approval process to assess residual risk before the resource is put into production. Each phase of the TSLC has corresponding security activities that must be performed to maintain a secure environment and comply with Postal Service policies and legal requirements. (See Handbook AS-805-A, *Information Resource Certification and Accreditation Process*, for more details.)

8-4.1 What the C&A Process Covers

The C&A process consists of seven interrelated phases that are conducted concurrently with the development and deployment of new information resources. The objectives of the C&A are to assess threats, define security requirements and controls, test security solutions, and evaluate the security controls and processes chosen to protect the information resource.

For sensitive-enhanced, sensitive, and critical resources must complete the full C&A process culminating with the certification, accreditation, and approval to deploy the information resource. All three approvals (i.e., certification, accreditation, and approval to deploy) are required before beginning operations.

All wireless information resources, regardless of sensitivity or criticality, must complete the full C&A process.

8-4.2 When C&A Is Required

The C&A is required for the following:

a. All information resources, regardless of whether they are located at a Postal Service or non-Postal Service facility or whether they are controlled directly by the Postal Service or through a contractor or business partner.

b. Pilot projects or proofs of concept for information systems prior to implementation to ensure that the project does not inadvertently expose the Postal Service to unnecessary security threats.

c. The frequency for recertification and reaccreditation is defined in the Re-Initiate C&A section.

8-4.3 Value of C&A Process to the Postal Service

C&A demonstrates that the Postal Service has taken due care to protect its information resources in accordance with policies and legal requirements defined by its business, legal, and administrative entities and ensures that

the security measures implemented to protect such resources are documented.

8-4.4 Access to Information Resources and Related Documentation

During the C&A process, the manager, CISO, or designated agent has unrestricted access to the information resources and related documentation.

8-4.5 Independent Processes

Independent processes are evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information resources. The following independent processes are conducted by an organization that is separate and distinct from those responsible for the development and operation of the information resource and that strictly adheres to the separation of duties policy:

a. Independent risk assessment.

b. Independent security code review.

c. Independent penetration testing and vulnerability scans.

d. Independent security test validation.

Additional information is available in Handbook AS-805-A, Information Resource Certification and Accreditation Process.

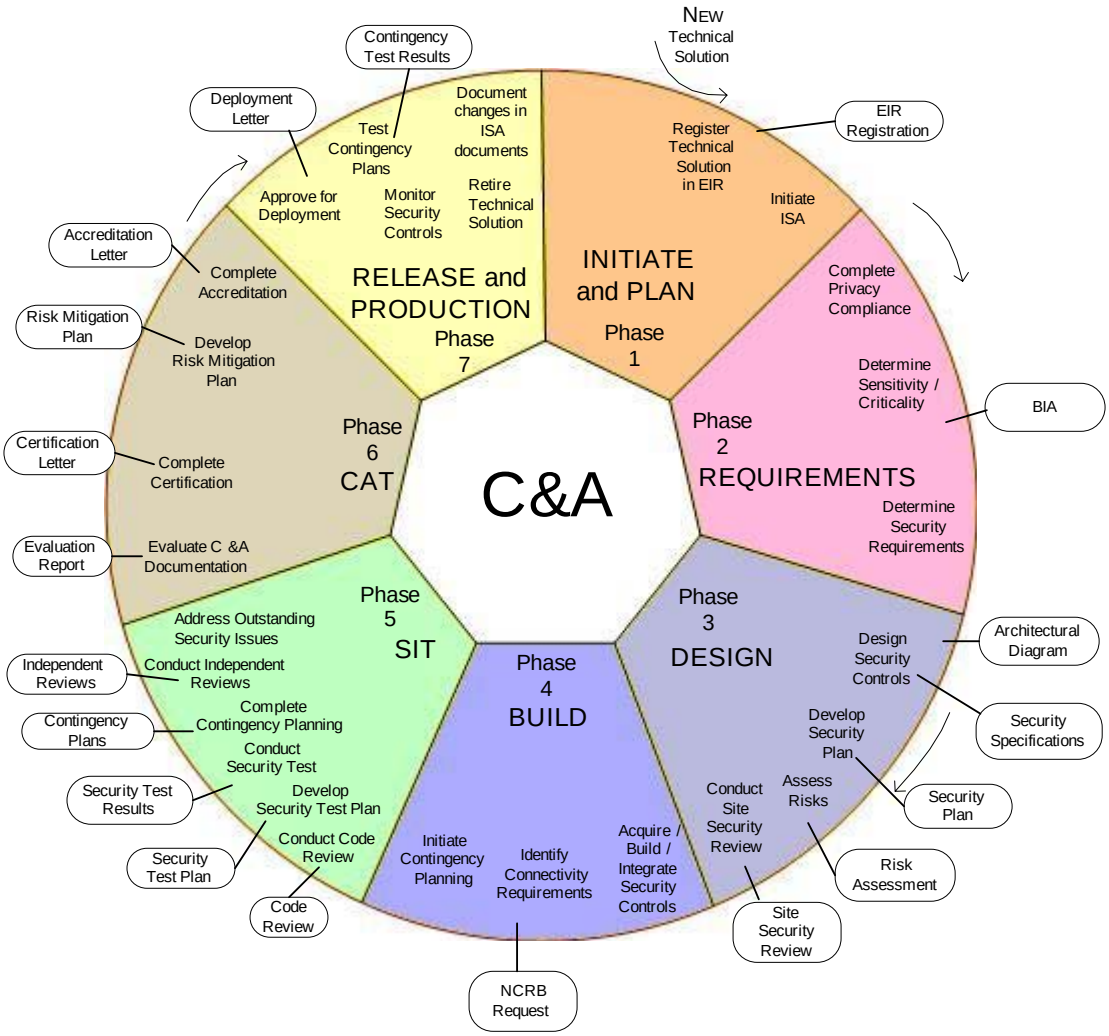
8-4.6 Contractual Terms and Conditions

Contract language and partnering agreements must reflect the information security requirements of the Postal Service defined in the C&A process. The executive sponsor is responsible for ensuring that the security requirements are included in all contracts that involve developing information resources and all contracts with businesses that transmit information to or from trusted Postal Service networks.

8-5 Information Resource C&A

Exhibit 8-5 depicts the seven phases and the major documents (deliverables) for each phase. The purpose and information security activities associated with the C&A phases are described in the following paragraphs.

Exhibit 8-5
Seven C&A Phases



8-5.1 Phase 1 — Initiate and Plan

Phase 1 determines what will be required during the C&A and the magnitude of the effort needed to complete the C&A process. The process is initiated for all information resources regardless of their location or whether they are controlled directly by the Postal Service or through a contractor or business partner. Information resources may be referred to as a technical solution within the TSLC. The C&A process can be applied to pilot, new, and production applications, infrastructure, and business partner initiatives.

8-5.2 Phase 2 — Requirements

Phase 2 determines the information security requirements and begins to assess the risks. The information security activities of Phase 2 are described in the following paragraphs.

8-5.2.1 Conduct Business Impact Assessment

A business impact assessment (BIA) is completed to determine the level of sensitivity and criticality and the information security requirements for the information resource.

8-5.2.1.1 Determine Sensitivity and Criticality

The Privacy Impact Assessment is completed along with the process to determine sensitivity and criticality all information resources.

8-5.2.1.2 Determine Security Requirements

Security requirements are defined for all information resources to secure the information resources commensurate with the risk. Security requirements include the following:

a. Baseline security requirements for all information resources.

b. Additional security requirements based upon the sensitivity and criticality of the information resource, legislation, regulations, directives, and industry requirements.

c. Additional conditional requirements based on request by senior management or specific criteria.

d. Additional security requirements recommended by the information system security officer (ISSO) based on generally accepted industry practices, the operating environment, and the risks associated with the information resource.

8-5.3 Phase 3 — Design

Based on the security requirements from the BIA, the security controls and processes for the information resource are defined. The information security activities of Phase 3 are described in the following paragraphs.

8-5.3.1 Develop High-Level Architecture

A high-level architectural diagram is developed and maintained current for all information resources documenting hardware, communication services and ports used, security devices, and interconnected resources. The architectural diagram is used by the manager, CISO ISS to determine the impact on the infrastructure and the need for additional security controls such as an enclave (see 11-3.7, Determining When a Secure Enclave Is Required).

8-5.3.2 Document Security Specifications

If information resource is contracted, security specifications are documented to satisfy the security requirements defined by the BIA.

8-5.3.3 Select and Design Security Controls

Identify potential security controls (safeguards) based on the information security requirements and in light of business requirements including project schedule and budget.

An analysis of potential controls is conducted to determine their potential effectiveness to remove, transfer, or otherwise mitigate risk to information resources. The controls analysis identifies any residual risk to the information resource.

A cost-benefit analysis is performed and documented to facilitate the implementation of cost-effective protection for information resources.

Safeguards are selected or designed based on the controls analysis and the cost-benefit analysis.

8-5.3.4 Develop Security Plan

A security plan must be developed for sensitive-enhanced, sensitive, and critical information resources. A security plan is also required for major information resources and general support systems. A security plan is a blueprint for designing, building, and maintaining an information resource that can be defended against threats, including intruders, both internal and external. The security plan covers both the development and production environment and describes all information security controls that have been implemented or planned.

8-5.3.5 Conduct Risk Assessment

A risk assessment must be conducted for all information resources to identify security concerns (e.g., threats, vulnerabilities, and control weaknesses), risk ranking, additional countermeasures, and residual risk (see 4-3, Information Resource Risk Management). The risk assessment can be started in this phase but must be updated throughout the TSLC.

8-5.3.6 Conduct a Site Security Review

The site security review assesses the physical security controls of facilities hosting sensitive-enhanced, sensitive, and critical information resources. The lack of adequate physical security controls could affect the availability, confidentiality, and integrity of Postal Service applications and the information resources hosting them.

8-5.4 Phase 4 — Build

The security controls and processes selected and defined in Phase 3 for the information resources are implemented in this Phase. The information security activities of Phase 4 are described below.

8-5.4.1 Develop, Acquire, and Integrate Security Controls

Appropriate security controls are developed in house, acquired, or outsourced depending on the cost-benefit analysis and integrated into the information resources and related processes.

8-5.4.2 Harden Information Resources

Information resources hosting sensitive-enhanced, sensitive, and critical applications and information resources that are part of the Postal Service infrastructure must be hardened to meet or exceed the requirements

documented in Postal Service hardening standards. Hardening refers to the process of implementing additional software, hardware, or physical security controls.

8-5.4.3 Develop Security Operating Procedures

Security operating procedures for emergencies, separation of duties, secure computer operations, manual processes, etc., must be developed for all information resources.

8-5.4.4 Develop Operational Security Training

Appropriate materials are developed for training users, system administrators, managers, and other personnel on the correct use of the information resource and its security controls.

8-5.4.5 Register Information Resource in eAccess

Register the information resource in eAccess, which is the Postal Service application for managing the authorization process for personnel needing to access the information resource and the associated information. Registration is also required for the use of managed accounts (e.g., machine accounts).

8-5.4.6 Develop Business Continuity and Facility Plans

Business continuity plans must be developed for critical information resources. A facility recovery plan is developed for facilities designated by the vice president Information Technology Operations as major information technology sites. These plans are started during this phase and updated in Phase 5 – System Integration Testing.

8-5.4.7 Identify Connectivity Requirements

Requirements for connectivity to the Postal Service infrastructure must be identified and a request must be submitted to the Network Connectivity Review Board (NCRB).

8-5.5 Phase 5 — System Integration Testing

The security controls and processes implemented in Phase 4 are tested. The information security activities of Phase 5 are described in the following paragraphs.

8-5.5.1 Develop Security Test Plan

A security test plan must be developed for sensitive-enhanced, sensitive, and critical information resources. A security test plan is also required for major information resources and general support systems. The security test plan evaluates the technical and nontechnical security controls and other safeguards to establish the extent to which the information resource meets the security requirements for its mission and operational environment.

8-5.5.2 Conduct Security Test and Document Results

Security testing is conducted using the approved security test plan. If a modification to a control is required, the change should be reflected in the security plan and the security test plan before the test is executed.

The results of the testing must be documented and communicated in language that is understandable to business-process owners and the ISSO.

8-5.5.3 Conduct Security Code Review

To protect the infrastructure, a documented security code review maybe required. (See Handbook AS-805-A for the criteria for conducting a code review.)

The security code review is based on the Postal Service Security Code Review Standards or an acceptable equivalent. This security code review is not required if an independent security code review is conducted.

8-5.5.4 Conduct Operational Security Training

Using the training materials developed in the prior phase, users, system administrators, managers, and other personnel are trained on the correct use of the information resource and its security safeguards.

8-5.5.5 Conduct Vulnerability Scan

A vulnerability scan is recommended for all information resources. A quarterly vulnerability scan is required for PCI applications and an annual vulnerability scan is required for externally facing applications. The scanning procedure must ensure adequate scan coverage and the updating of a list of vulnerabilities.

8-5.5.6 Conduct Independent Risk Assessment

An independent information security risk assessment may be required to evaluate the appropriateness and effectiveness of the security controls and identify residual risk. (See Handbook AS-805-A for the criteria for conducting an independent risk assessment.)

8-5.5.7 Conduct Independent Security Code Review

Information resources may be subject to an independent code review of the source code and documentation to verify compliance with software design documentation and programming standards and the absence of malicious code. The independent code review may also evaluate correctness and specific security issues. (See Handbook AS-805-A for the criteria for conducting an independent security code review.)

8-5.5.8 Conduct Independent Penetration Testing and Vulnerability Scans

Independent penetration testing evaluates the effectiveness of the implemented information resource configuration. Vulnerability scans evaluate information resources for vulnerabilities and compliance with Postal Service information security policies and standards. (See Handbook AS-805-A for the criteria for conducting independent penetration testing and vulnerability scans.)

8-5.5.9 Conduct Independent Validation of Security Testing

The independent security test validation addresses the appropriateness and effectiveness of the security controls and corroborates the previously conducted security test results. The scope of the independent security test validation depends on the information resource, its environment, and the associated threats and vulnerabilities. The independent security test validation is usually carried out at the development or test site.
(See Handbook AS-805-A for the criteria for conducting an independent security test validation.)

8-5.5.10 Conduct Development of Contingency Plans

The contingency plans (and, if applicable, the facility recovery plan) from Phase 4 – Build must be updated as required.

8-5.6 Phase 6 — Customer Acceptance Testing

Phase 6 consists of activities described below that culminate in the certification, risk mitigation plan, accreditation, acceptance of residual risk, and approval to deploy an information resource.

8-5.6.1 Project Manager Develops C&A Documentation Package

Sensitive-enhanced, sensitive, and critical information resources require a C&A documentation package. The package is a consolidation of the designation of sensitivity and criticality and associated protection requirements (BIA); threats, vulnerabilities, additional controls, and residual risks (risk assessment); protection mechanisms (security plan and business continuity plans); and the security test and evaluation results.

8-5.6.2 ISSO Reviews C&A Documentation Package and Prepares Evaluation Report

The ISSO reviews the C&A documentation package and prepares a C&A evaluation report highlighting the findings and recommendations. The ISSO escalates security concerns or forwards the C&A evaluation report and supporting documentation to the certifier for review.

8-5.6.3 Certifier Escalates Security Concerns or Certifies Information Resource

The certifier (e.g., manager, C&A process) reviews the C&A evaluation report and the supporting C&A documentation package, escalates security concerns or prepares and signs a certification letter, and forwards the certification letter and C&A documentation package to the portfolio manager.

If the certifier decides not to certify the information resource, he or she will indicate the C&A Phase to return to for rework.

8-5.6.4 Portfolio Manager Escalates Security Concerns or Prepares Risk Mitigation Plan

The portfolio manager reviews the certification letter and the supporting C&A and business documentation and escalates security concerns or prepares a risk mitigation plan for any residual risks rated as medium or high,

recommending whether the risks should be accepted, transferred, or further mitigated. The portfolio manager then forwards the risk mitigation plan and C&A documentation package to the accreditor.

If the portfolio manager decides not to proceed toward accreditation, he or she will indicate the C&A phase to return to for rework.

8-5.6.5 Accreditor Escalates Security Concerns or Accredits Information Resource

The accreditor (e.g., manager, CISO) reviews the risk mitigation plan and the supporting C&A documentation, escalates security concerns or prepares and signs an accreditation letter, and forwards the accreditation letter and final C&A documentation package to the executive sponsor and portfolio manager.

If the accreditor decides not to accredit the information resource, he or she will indicate the C&A phase to return to for rework.

8-5.7 Phase 7 — Release and Production

Phase 7 is the operation and maintenance period of the information resource and includes activities to ensure that chosen security controls and procedures are functioning properly and that security controls are modified or added as needed to continue to protect the information resource. The information security activities for Phase 7 are described in the following paragraphs.

8-5.7.1 Executive Sponsor and Portfolio Manager Make Decision to Deploy (or Continue to Deploy) or Return for Rework

The executive sponsor and portfolio manager review the accreditation letter, risk mitigation plan, and supporting C&A documentation package. They will issue a joint decision on whether to accept the residual risk and approve the information resource for deployment with what restrictions, if any.

If they decide not to approve deployment, they will indicate the C&A Phase to return to for rework. If they decide to approve and deploy, they will prepare and sign an acceptance letter.

8-5.7.2 Data Conversion

A data conversion plan must be defined so that it incorporates collecting, converting, and verifying data for completeness and integrity and resolving any errors found during conversion. Create a backup of all data prior to conversion and maintain audit trails to track the conversion to ensure there is a fallback and recovery plan in case the conversion fails. Ensure that the backed-up data conforms to the applicable data retention schedule.

8-5.7.3 Deploy Information Resource

All three approvals (i.e., certification, accreditation, and approval to deploy) are required before deploying the information resource. When the information resource is deployed, the security controls for the information resource are implemented as documented in the security plan and with the caveats included in the acceptance letter.

8-5.7.4 Information Resource Maintenance

Information resources must be maintained in a timely manner. The tools, techniques, and mechanisms used to maintain information resources must be properly controlled.

8-5.7.5 Follow Security-Related Plans and Continually Monitor Operations

The security-related plans must be followed during deployment, operation, and maintenance. The information resource controls must be continually monitored by the project team to ensure they are working as intended and remain in compliance with the security-related plans.

8-5.7.6 Periodically Review, Test, and Audit

Information resources are periodically reviewed, tested, and audited for compliance with Postal Service policies (e.g., plans related to facility recovery or business continuity are tested to ensure that these plans meet business and security objectives).

For non-PCI information resources, a subset of the information security controls must be formally tested annually by the project team, the tests documented, and the results submitted to the applicable ISSO. The security controls that are volatile or critical to protecting the information system must be assessed at least annually. All other controls must be assessed at least once during the information resource's 3-year accreditation cycle (e.g., one third of these other controls each year).

8-5.7.7 Reassess Risks and Upgrade Security Controls

Risks are re-assessed as part of the re-initiation of the C&A process. Security controls are upgraded as necessary to protect the information resource and assure business continuity.

8-5.7.8 Update Security-Related Plans

Security-related plans are updated in response to changing environment, changing technology, re-assessed risks or vulnerabilities, and as part of the re-initiation of the C&A process.

8-5.7.9 Re-Initiate C&A

Re-initiating the C&A is required:

- Every year for PCI information resources and selected information resources designated by the manager, CISO.
- Every 3 years for sensitive-enhanced, sensitive, and critical information resources not addressed above.
- Every 5 years for all other information resources (i.e., nonsensitive and noncritical).

Re-initiating the C&A may result in recertification, re-accreditation, re-acceptance of risk, and re-approval for deployment. Re-initiating the C&A could also be required for the following reasons:

a. Significant changes to the operating environment or the business requirements of the information resource. Significant changes may include, but are not limited to:
   (1) Change in the functions of the information resource or data that alters the criticality or sensitivity designation of the information resource.
   (2) Change from one major information resource to another, such as BroadVision to WebObjects.
   (3) Change from one database information resource to another, such as Oracle to MS–SQL.
   (4) Change in the hosting location, such as from a Postal Service facility to an outsourced, non–Postal Service location.
   (5) Change in the operating environment resulting from discovery of a new vulnerability or threat that significantly alters the risk to the information resource.

b. A significant information security incident that violates an explicit or implied security policy, compromising the integrity, availability, or confidentiality of an information resource (e.g., a critical disruption or monetary loss, the unauthorized modification of sensitivity or criticality information, or the release of sensitive-enhanced, sensitive, information).

c. A significant finding of an audit or other external assessment.

d. A request by the CIO; VP IT Operations; the manager, CISO; the vice president of the functional business area; or the executive sponsor.

8-5.7.10 Retire Information Resource

8-5.7.10.1 Dispose of Data

All Postal Service sensitive-enhanced and sensitive information that is no longer needed, whether in electronic or nonelectronic format, is transferred, archived, or destroyed in accordance with official Postal Service policies and procedures (see 3-5.8, Disposal and Destruction of Information and Media, and Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management)*.

8-5.7.10.2 Sanitize Equipment and Media

All Postal Service sensitive-enhanced and sensitive information is completely erased or destroyed prior to disposal of the hardware or electronic media on which it resides (see 3-5.8, Disposal and Destruction of Information and Media).

9 Information Security Services

9-1 Policy

Information security services provide the policies, requirements, standards, and processes that enable the integration and implementation of information security across Postal Service information resources to ensure a viable secure computing infrastructure and to protect information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction.

All Postal Service personnel must adhere to the following information security services:

a. Authorization.
b. Accountability.
c. Identification.
d. Authentication.
e. Confidentiality.
f. Integrity.
g. Availability.
h. Security administration.
i. Audit logging.

9-2 Security Services Overview

Information security services provide the framework for implementing information security measures used to protect information resources. Security services are as follows:

a. Authorization determines whether, and to what extent, personnel should have access to specific computer resources.
b. Accountability associates each unique identifier with one user or system process to enable tracking of all actions by the user or of the process on the information resource.
c. Identification associates a user with a unique identifier (i.e., user account or logon ID) by which that user is held accountable for the actions and events initiated by the identifier.
d. Authentication verifies the claimed identify of an individual, workstation, or originator.

e. Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

f. Integrity ensures the correct operation of information resources, consistency of data structures, and accuracy of stored information.

g. Availability ensures information resources are accessible by authorized personnel or other information resources when required.

h. Security administration implements management constraints, operational procedures, and supplemental controls established to provide adequate protection of an information resource.

i. Audit logging records operational and security-related events.

9-3 Authorization

Authorization provides the framework for determining whether, and to what extent, personnel should have access to computer resources. Information resources must be configured to ensure that no user is allowed access to an information resource (e.g., transaction, data, and process) unless authorized by appropriate Postal Service management. Upon employment, personnel may be granted access to temporary information services until they receive clearance.

9-3.1 Authorization Principles

Access must be granted based on personnel roles and the security principles of clearance, need to know, separation of duties, and least privilege.

9-3.1.1 Clearances

For personnel without clearances, access is restricted to temporary information services. Managers must use eAccess to request access authorization for individuals who do not have the appropriate clearance and are responsible for the access activities of those individuals.

9-3.1.2 Need to Know

For sensitive-enhanced, sensitive, and critical information resources access must be limited in a manner that is sufficient to support approved business functions. Access to sensitive-enhanced and sensitive Postal Service information resources must be limited to personnel who need to know the information to perform their duties.

9-3.1.3 Separation of Duties

Only authorized personnel are approved for access to Postal Service information resources. This approval must be specific to an individual's roles and responsibilities in the performance of his or her duties and must specify the type of access (e.g., read, write, delete, and execute); specific resources and information; and time periods for which the approval is valid. Separation of duties and responsibilities are considered when defining roles.

9-3.1.4 Least Privilege

For sensitive-enhanced, sensitive and critical information resources access is based on providing personnel with the minimum level of information resources and system functionality needed to perform their duties. Systems and applications must define as many levels of access as necessary to prevent misuse of system resources and protect the integrity and confidentiality of Postal Service information. Postal Service information resources must be capable of imposing access control based on specific functions (e.g., create, read, update, delete, and execute).

9-3.2 Authorization Management

eAccess is the Postal Service application for managing authorization to information resources. eAccess centralizes the management of user identities and access rights over the entire life cycle from hiring to termination.

9-3.2.1 Requesting Authorization

All requests for authorization to access Postal Service information resources, including temporary information services, must be requested via eAccess at *https://eaccess*.

9-3.2.2 Temporary Information Services

Requests for temporary information services must go through eAccess for proper management approval. For contractor personnel who have submitted their security clearance documentation, the manager, Corporate Information Security Office (CISO), may authorize temporary access to the following information services until the contractor's security clearance is issued:

a. ACE active directory account.

b. E-mail access.

c. Office suite of services.

d. Intranet browser access.

The following information services are unavailable under temporary access:

a. Internet browser access.

b. Remote access.

c. Access to e-mail except within the Postal Service intranet.

Note: No access beyond temporary information services will be authorized until the appropriate personnel security clearance is granted. Upon receipt of an appropriate security clearance, individuals requiring access beyond temporary information services may request additional authorization via eAccess.

9-3.2.3 Expiration of Temporary Access Authorization

Temporary access expires in 3 months.

9-3.2.4 Approving Requests

All requests for authorization must be approved by the individual's manager or supervisor, the contracting officer's representative (if the request is for a contractor), and the executive sponsor of the application.

9-3.2.5 Periodic Review of Access Authorization

On a semiannual basis, managers must review access granted to personnel under their supervision to ensure that the access is still required for personnel to perform their duties. The manager must keep a record of the review.

The manager CISO may require that some privileged system/application accounts be reconciled to related eAccess records on a monthly basis. Discrepancies must be investigated and resolved in a timely manner.

9-3.2.6 Implementing Changes

System administrators and database administrators must implement all approved authorization requests for the information resources under their control. They must not add, modify, or revoke access to information resources except in accordance with Postal Service policies.

9-3.2.7 Revoking Access

All managers must ensure that access to information resources is immediately revoked for personnel when no longer required because of a change in job responsibilities, transfer, or termination. The manager will advise the system and/or database administrators as to the final disposition of files and data.

9-3.2.8 User Registration Management

User registration management must provide the following functionality to allow managers to perform their roles and responsibilities in the authorization process:

a. Register user to information resources.

b. Assign unique identifier.

c. Track modifications to user access authorizations.

d. Provide management reports.

e. Validate user identity.

f. Revoke user access.

g. Log and audit access requests.

9-3.2.9 Emergency Access

In instances during which an individual has possession of Postal Service information that is required by his or her manager and the individual is unavailable, the following process must be followed:

a. The individual's manager initiates a request for access to the information using a documented procedure (e.g., remedy or information ticket). The individual's manager is accountable for the emergency access.

b. Audit logging for all activities related to an emergency access request is required and must be protected and retained according to Postal Service standards.

c. The emergency access must be conducted under the identity of the user authorized by the manager and actually performing the access. Under no circumstance will the unavailable individual's logon ID or password be used or compromised in an emergency access.

d. The system administrator either rewrites the access rules giving the manager or the manager's designee access to the information (files), or the system administrator is authorized by the manager to access the information on the manager's behalf.

e. Upon completion of the emergency access, all access to the information is returned to its original state.

f. The unavailable individual is notified of the emergency access as soon as he or she becomes available.

9-3.3 Authorization Requirements

Information resources must comply with authorization requirements including, but not limited to, the following:

a. The information resource must not allow access to resources without invoking the authorization process and checking the assigned rights and privileges of the authenticated user.

b. The information resource must have features to assign user privileges (i.e., access permissions) to logon IDs, roles, groups, and information resources.

c. Privileges on information resources (e.g., workstations, consoles, terminals, and subsidiary networks) must not allow the user to bypass or upgrade his or her privileges established in centralized access control lists or databases.

d. The information resource must have the capability to restrict session establishment or information resource access based on time of day, day of the week, calendar date of the login, and source of the connection. Information resources running on operating systems that do not have these capabilities must implement compensating controls (e.g., monitoring devices).

e. The information resource must provide the administrator-configurable capability to limit the number of concurrent logon sessions for a given user.

f. The information resource must not offer any mechanism to bypass authorization restrictions.

9-4 Accountability

Accountability is the process of associating any action on the information resource with one and only one user, process, or other information resource and is essential for maintaining minimum levels of information security.

9-4.1 Types of Accountability

Accountability for access to information resources must be established at the site, network, and the individual level.

9-4.1.1 Site Accountability

Site accountability associates users or information resources with a specific location. Site accountability is established by issuing a site identification number or code (site ID) that is restricted by system hardware or software to a unique system, network, or terminal address in a controlled environment.

9-4.1.2 Network Accountability

Network accountability associates users or information resources with a specific network or logical subnet to a network. Network accountability is established by issuing a network identification number or code (network ID) or through the network address.

Individual Accountability

Individual accountability associates each user or information resource (e.g., a workstation or terminal) with any action on an information resource. Individual accountability is established by issuing a unique user or logon identification number or code (i.e., user ID or logon ID). Machine accountability may be established for a specific information resource through its workstation address or other identifier. All information resources must be capable of individual accountability and must do the following:

a. Identify users each time they attempt to logon to the system.

b. Verify that users are authorized to use the system.

c. Associate all actions taken by a user with the user's unique identifier (i.e., user ID or logon ID).

9-4.2 Types of Accounts

Access to information resources is managed through the use of multiple types of accounts, including the following:

a. User.

b. Privileged.

c. Machine.

d. Shared.

e. Vendor default and maintenance.

f. Guest.

Ownership for privileged, shared, and maintenance logon IDs must be documented and administered in a secured manner.

9-4.2.1 User Accounts

User accounts provide application/platform users with a minimum level of information resources and application functionality needed to perform their duties (i.e., least privilege) and do not carry special privileges above those required to perform the user's business function. This includes limited access accounts that exist for a specific purpose (e.g., an auditor account).

Application user accounts are used to log into the application via a front-end interface, and the account privileges and roles are restricted by the approved access. Platform user accounts (i.e., database and operating system) are used to access platform-level resources and are limited to nonprivileged access rights.

9-4.2.2 Privileged Accounts

Privileged accounts (e.g., administrator or maintenance accounts) are application- or platform-level (i.e., database and operating system) accounts that have higher levels of rights such as account creation/update/deletion, full application/platform functionality, or a subset of rights that have been designated as privileged. Assignment must be restricted to a unique individual whose duties require these additional privileges. Use is restricted to performing those job functions required by the privileged account; individuals must use their regular user accounts to perform nonprivileged functions. An audit trail must be maintained on all privileged account usage.

9-4.2.3 Machine Accounts

Machine accounts are assigned to an information resource (e.g., server/application) or other automated process/service (not an individual) used to process data and/or identify actions or requests. Machine accounts must be placed under management control. Machine accounts must be created with the minimum access rights and privileges required to perform the necessary business function. These accounts must not be allowed root or administrative privileges. The accounts are managed by the Postal Service entity responsible for the life cycle of the account from creation, deployment, usage, and retirement when no longer needed.

9-4.2.4 Shared Accounts

Shared accounts have a single logon ID that is used by more than one individual. This approach to account usage is highly discouraged and requires the appropriate level of management approval via eAccess. The use of shared accounts must be tracked (e.g., logged) to manage individual accountability. The requesting manager is responsible for undocumented usage of the shared accounts and is responsible for password management. Shared training accounts must not include access to Postal Service production systems.

9-4.2.5 Vendor Default and Maintenance Accounts

Vendor default accounts shipped and/or pre-installed on a vendor product must be removed or disabled. Vendor maintenance accounts must be enabled only when needed and controlled by a responsible Postal Service entity.

9-4.2.6 Guest Accounts

Guest accounts are not allowed for access to Postal Service network information resources. Guest accounts expose information resources to risk by allowing access to information resources through the use of a generic logon ID that either uses no password or a widely known password. Guest accounts incorporated into any software or established through any other

means must be deleted or disabled. This policy does not apply to guest networks isolated from the Postal Service intranet that are used to support non-Postal Service external access.

9-4.3 Account Management

Accounts must be established in a manner that ensures access is granted on clearances, need to know, separation of duties, and least privilege basis.

9-4.3.1 Establishing Accounts

To establish an account, personnel must request an account from their manager or supervisor via eAccess at *https://eaccess*.

9-4.3.2 Documenting Account Information

The account information, or database, must contain the following information for each user account: logon ID, group memberships, access control privileges, authentication information, and security-relevant roles. Any security-related attributes that are maintained must be stored securely to protect their confidentiality and integrity.

9-4.3.3 Configuring Account Time-Outs

Accounts must be configured to log the workstation off the network or disable the session after a predetermined period of inactivity and enforce re-authentication. This requirement should be automated where possible. The Postal Service default standard period of inactivity is a maximum of 30 minutes. This action reduces the amount of time Postal Service information resources are vulnerable to compromise. Any deviation from this standard is the responsibility of the executive sponsor and must be documented and approved by the CISO.

9-4.3.4 Departing Personnel

Accounts must be deleted or passwords changed when personnel leave the organization.

9-4.3.5 Vendor Maintenance Accounts

Vendor maintenance accounts must be managed, enabled only when needed by the vendor, and monitored while being used.

9-4.3.6 Handling Compromised Accounts

Information resources must provide automated mechanisms to support identifying and handling information security incidents. All personnel who suspect an account has been compromised must immediately notify management and follow the incident reporting process (see 13-3.2, Incident Reporting).

9-5 Identification

Identification is the process of associating a person or information resource with a unique enterprisewide identifier (e.g., a user logon ID). The logon ID is used in conjunction with other security services, such as authentication measures, to track activities and hold users accountable for their actions. Users are responsible for all actions performed on Postal Service information resources under their logon ID.

Identification requirements for processing and control devices in the mail processing and mail handling equipment (MPE/MHE) environment for private nonroutable network address space are defined by Engineering.

9-5.1 Issuing Logon IDs

Logon IDs or user IDs are unique groups of letters, numbers, or symbols assigned to a specific person or information resource. All personnel using Postal Service information resources are issued a logon ID in conjunction with the authorization process. No two users are assigned the same logon ID. This policy does not apply to users of managed shared accounts.

9-5.2 Protecting Logon IDs

Logon IDs must be protected in accordance with the following:

a. Personnel must not share their logon IDs or permit others to use them to access Postal Service information resources.

b. Logon IDs must not be embedded in application code or batch files or stored in application files or tables unless approved compensating security controls are implemented.

9-5.3 Suspending Logon IDs

After six unsuccessful attempts to log on to an information resource, the logon ID or account must be suspended for a period of at least 5 minutes. If the logon ID or account does not unsuspend itself after the suspension period, the user must use ePassword Reset or call the Help Desk and follow defined procedures for resolution. Logon IDs not used within the last 180 days must be disabled.

9-5.4 Failed Logon Attempts

9-5.4.1 Recording Failed Logon Attempts

Failed logon attempts must be recorded for audit trail and incident reporting purposes.

9-5.4.2 User Notification of Failed Logon Attempt

Notification to the user of a failed logon attempt will reflect only that the logon failed. The reason for the failed logon attempt and information previously entered, including the disguised or clear password, must not be returned to the user.

9-5.5 Terminating Logon IDs

Logon IDs not used in the last year must be deleted.

9-5.6 Identification Requirements

Information resources must comply with security requirements including, but not limited to, the following:

a. The information resource must, at a minimum, use logon IDs as the primary means of identification.

b. The information resource must have the capability to automatically disable a logon ID that has not been used for an administrator-configurable period of time.

c. The information resource must not allow an administrator to create, intentionally or inadvertently, a logon ID that already exists.

d. A logon ID must not exist without associated authentication information.

e. The information resource must not provide any process to bypass the authentication information for any logon ID.

f. The information resource must have the capability of associating each internal process with the logon ID of the user who initiated the process. Processes that are not initiated by a user, such as print spoolers, database management servers and any spawned subprocesses, must be associated with an identifier code, such as “system ownership.”

9-6 Authentication

Authentication is the process of verifying the claimed identity of an individual, workstation, or originator. While identification is accomplished through a logon ID, authentication is achieved when the user provides the correct password, personal identification number (PIN), or other authenticator associated with that identifier. Personnel must be required to identify and authenticate themselves to the information resource before being allowed to perform any other actions. Authentication requirements for processing and control devices in the MPE/MHE private nonroutable network address space are defined by Engineering. Means of authentication, or authenticators, may include the following:

a. Passwords.

b. Personal identification numbers.

c. Shared secrets.

d. Digital certificates and signatures.

e. Smart cards and tokens.

f. Biometrics.

g. Strong authentication.

9-6.1 Passwords

Passwords are unique strings of characters that personnel or information resources provide in conjunction with a logon ID to gain access to an information resource. Passwords, which are the first line of defense for the protection of Postal Service information resources, must be treated as sensitive information and must not be disclosed.

9-6.1.1 Password Selection Requirements

Password requirements must comply with the following:

a. For all users, passwords must consist of at least eight characters and contain at least one character from three of the four following types of characters: English uppercase letters (A–Z), English lowercase letters (a-z), Westernized Arabic numerals (0–9), and nonalphanumeric characters (i.e., special characters such as &, #, and $). It is recommended that system administrators use two-factor authentication.

b. The only exception to the standard password requirements is as follows: Mainframe passwords must consist of at least seven characters and contain at least one character from the following types of characters: alphabetic characters, Westernized Arabic numerals (0–9), and nonalphanumeric characters (@, # or $). It is recommended that mainframe user passwords contain English uppercase and lowercase letters.

c. For all users, passwords must not contain the user's name or any part of the user's full name.

d. Passwords must not be repeated (reused) for at least five generations.

9-6.1.2 Password Selection Recommendations

The following password recommendations are prudent security practices intended to enhance the password complexity and protect the password from attempted password cracking:

a. Do not use family member names or other information easily discovered about the user (e.g., license plate number, phone number, birth date, and street name).

b. Do not use commonly used words such as words that appear in the dictionary or Postal Service terminology.

c. Do not use all the same characters or digits or other commonly used or easily guessed formats.

d. Use longer password conventions whenever possible (e.g., pass-phrases and run-on multiword strings).

9-6.1.3 Initial Password

Passwords must always be delivered in a secure manner. The initial password for users must be sent via protected electronic delivery system or personal delivery to the user (First Class Mail is also acceptable). For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at logon.

Note: Caution must be taken not to standardize on generic or global passwords when issuing new accounts or when resetting forgotten passwords.

9-6.1.4 Password Suspension

After six unsuccessful attempts, suspend the account.

9-6.1.5 Reset Passwords

Users with nonprivileged accounts who have forgotten their passwords or need to perform routine password resets, should reset their password by invoking ePassword Reset. The exception to using the ePassword Reset system is for privileged, machine and vendor default accounts (see below). The ePassword Reset system requires user authentication prior to allowing the user to perform a password reset. If a user calls the Help Desk to reset a password, users are challenged by Help Desk personnel to provide further confirmation of identity prior to resetting the password. Password change requests via the Help Desk are documented via a change request ticket. The password is reset to a temporary password by an administrative group, and the user must then change the password at first logon.

ePassword Reset is not used for privileged, machine, and vendor default accounts. The passwords to these accounts are changed by the system administrator group via the Help Desk. When users of these accounts request the reset of a password, the users are challenged by Help Desk personnel to provide further confirmation of their identity (e.g., some predetermined shared secret that only the user would know) prior to resetting the password. Upon confirmation of user identity, the request is documented via a change request ticket and assigned to the appropriate administrator group for resetting the password. For privileged accounts, the administrator group resets to a temporary password and the privileged user must then change the password at first logon.

9-6.1.6 Password Expiration

The information resource must offer an authentication information-aging feature that requires users to periodically change authentication information, such as passwords. All Postal Service personnel must change their passwords when prompted by the system or risk being locked out, thus requiring assistance to reset the account. Password expiration requirements are as follows:

a. Prior to the expiration of authentication information, such as passwords, the information resource provides notification to the user.

b. At least every 30 days, passwords for privileged accounts or for those accounts considered sensitive (e.g., system supervisors, software specialists, system administrators, or vendor-supplied) must be changed.

c. At least every 90 days, passwords for all other accounts must be aged and changed.

9-6.1.7 Requests for Use of Nonexpiring Password Accounts

All requests for use of nonexpiring password accounts must be submitted in writing (e-mail is acceptable) by the executive sponsor to the manager, CISO. These accounts are tracked for compliance purposes. The executive sponsor is accountable for the use of these accounts. If approval is granted, the following compensating controls must be implemented:

a. Account must be in a centrally managed database. No privileged access allowed.

b. Encrypt the LDAP call to keep the password from being transmitted across the network in clear text.

c. Change password when personnel with access to the account leave or transfer.

d. Nonexpiring password accounts must be requested and documented through eAccess.

e. Ownership of nonexpiring password accounts must be identified and recertified on a semi-annual basis.

f. Rights and privileges of nonexpiring password accounts must be reviewed at least on a semi-annual basis to evaluate the appropriateness of access.

g. Passwords for nonexpiring password accounts must use a complex password that exceeds standard length requirements.

h. Source-restrict the account to a specific host and do not allow console or remote entry.

i. Restrict access to the password to operations staff with a need to know.

9-6.1.8 Password Protection

Passwords used to connect to Postal Service information resources must be treated as sensitive information and not be disclosed to anyone other than the authorized user, including system administrators and technical support staff. Requirements for protecting passwords include the following:

a. Passwords must not be shared except those used for shared accounts.

b. If passwords are written down and stored outside the user's personal control, they must be secured in a tamper-resistant manner (e.g., an envelope with registry seal, time stamped, and signed by the user) to ensure that any disclosure or removal of the written password is clearly recognizable.

c. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user or has been otherwise compromised, the user must immediately change the password.

d. Passwords must be encrypted in transit.

9-6.1.9 Password Storage

Passwords must be stored in one-way encrypted format. This includes passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems.

9-6.1.10 Vendor Default Passwords

Vendor-supplied default accounts must be disabled, removed, or the passwords must be changed before connecting the system or introducing the software to the Postal Service network. This includes passwords used by contractors or consultants when configuring a system.

9-6.1.11 Password Requirements

Information resources must support the following password requirements:

a. Deny access if the user does not comply with password selection or expiration criteria.

b. Set initial password to a temporary password and require user to change the temporary password on first logon.

c. Suspend account after an administrator-configurable number of unsuccessful entries.

d. Require re-authentication by the user, as well as reconfirmation of the new password, at the time of an attempted password change.

e. Store passwords in a one-way encrypted format.

f. Encrypt passwords in transmissions.

g. Require users to periodically change passwords (password aging).

h. Change vendor-supplied default passwords prior to use.

9-6.2 Personal Identification Numbers

PINs are a specialized type of authenticator used for limited applications. PINs are used in conjunction with unique identifiers to authenticate users to information resources. Like passwords, PINs must be treated as sensitive information and must not be disclosed. All personnel must comply with Postal Service policies regarding PIN management and usage and are directly responsible for all actions taken using an assigned identifier and PIN.

9-6.2.1 PIN Generation and Selection Requirements

To ensure that PINs retain integrity and confidentiality, PINs must be protected during generation and dissemination. All personnel are encouraged to change their PIN from the initial assignment. PINs must:

a. Be a minimum of four characters in length, two of which are unique.

b. Avoid obvious combinations or sequences.

c. Avoid well-known or easily guessed combinations (e.g., social security number, telephone number, and house address).

9-6.2.2 PIN Distribution

Secure delivery methods include First Class Mail, an encrypted delivery system, or personal delivery to the user. New or replacement PINs must not be delivered by telephone, facsimile, or electronic mail to protect against unauthorized disclosure.

9-6.2.3 PIN Protection

PINs must be committed to memory or stored in a secure location. Information resources must store PIN data in an encrypted format that meets Postal Service encryption standards. All access, additions, modifications, and deletions to the PIN data must be logged and monitored. If PIN authentication is performed over an open network, such as the Internet, PINs must be encrypted during transmission according to Postal Service encryption standards.

9-6.2.4 Forgotten PINs

When requesting replacement of a forgotten PIN, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes. All forgotten PINs must be replaced

9-6.2.5 Suspension

When using a PIN for authentication, the information resource must be disconnected after three incorrect entries and the PIN account suspended after six incorrect entries. When a suspended PIN account is reactivated, the user must be assigned a new PIN that is delivered via secure methods.

9-6.2.6 PIN Cancellation and Destruction

A PIN suspected of compromise must be cancelled immediately and a new PIN generated and delivered via secure methods. Unauthorized users who no longer require access to the system must be removed immediately. All PIN data must be destroyed when the user no longer requires access to the system or leaves Postal Service employment.

9-6.2.7 PINs Used for Financial Transactions

PINs used for financial transactions must comply with American National Standards Institute Financial Services Technical Publication X9.8, PIN Management and Security. Financial transactions at high risk for fraud may not be suitable for reliance on PINs as the primary authentication mechanism.

9-6.3 Shared Secrets

A shared secret is an authentication mechanism used to re–set a user's password or PIN. When requesting the reset of a password or PIN, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes. Shared secrets must comply with the following:

a. Be a minimum of eight characters.

b. Be protected and stored as sensitive information.

c. Be stored encrypted if stored electronically.

d. Have the user's account suspended if the shared secret is entered incorrectly three times.

e. Ensure an information resource using shared secrets provides a secure process for recording an initial shared secret and changing the shared secret in the event of suspected compromise.

9-6.4 Digital Certificates and Signatures

A digital certificate contains a name, a public key, and a digital signature computed over the first two elements. The certificate's purpose is to relate a unique name to a specific public key and is used for encryption and decryption of files and the nonrepudiation of messages. The Postal Service sets standards for the properties, utilization, and acceptance of digital certificates in Postal Service systems and applications where digital certificates are used.

9-6.4.1 Digital Signature

A digital signature is a digital code that can be attached to an electronically transmitted message or file that uniquely identifies the sender. Digital certificates are required when using digital signatures. Digital signatures perform three important functions:

a. Integrity allows the recipient of a given message or file to detect whether that message or file has been modified.

b. Authentication makes it possible to verify cryptographically the identity of the person who signed a given message.

c. Nonrepudiation prevents the sender of a message from later claiming that they did not send the message.

9-6.4.2 Certificate and Signature Standards

Standards for digital certificate properties, utilization, acceptance, and practices can be found in the Postal Service Public Key Infrastructure (PKI) X.509 Certificate Policy (CP) and the Postal Service Subordinate Certificate Authority (CA) Certificate Practice Statement (CPS) that are on the Corporate Information Security Web site under Public Key Infrastructure (PKI). Standards established for the use, maintenance, and performance of cryptographic keys associated with digital certificates and signatures can be found in the section entitled, Key Management.

9-6.5 Smart Cards and Tokens

Smart cards and tokens are tangible objects that usually contain a built-in microprocessor to store and process information used to verify the identity of a user. Smart cards and tokens are valid methods of authentication. The CISO must approve all implementations of these technologies for accessing information resources. The CISO, in conjunction with the Inspection Service, sets standards for the use and protection of smart cards and tokens. Protect smart cards and tokens from theft and do not allow others to use them.

9-6.6 Biometrics

Using biometric information is a valid method of authentication. Biometrics are technologies used to authenticate individuals by means of unchanging biological characteristics (e.g., fingerprints, palm prints, voice prints, or facial, iris, and retina scans). The CISO must approve all implementations of biometric technologies for accessing information resources. Biometric information is sensitive-enhanced information and must be protected. The CISO, in conjunction with the Inspection Service, sets standards for the use of biometric authentication and the storage of biometric information.

9-6.7 Strong Authentication

Strong authentication consists of two-factor or multifactor authentication tools (e.g., smart card and PIN or thumbprint and password) that move toward the concept of nonrepudiation or conclusive tracing of an action to an individual. Single-factor authentication tools such as logon IDs and passwords do not provide strong authentication.

9-6.8 Nonrepudiation

Nonrepudiation is the security property that ensures that the sender cannot deny sending the message, the recipient cannot deny receiving the message, and actions can be conclusively traced to a specific individual. When required, an information resource must have the capability to support nonrepudiation.

9-6.8.1 Information Resource Nonrepudiation Requirements

Nonrepudiation requirements include the following:

a. The information resource must incorporate government- and industry-approved standards for digital signatures, key management, time stamping, and evidence archiving.

b. The information resource must facilitate nonrepudiation of transactions or communications by performing strong authentication of the associated parties and maintaining data integrity for related transactions or communications.

c. The information resource must have the capability to record and archive security-related events associated with a specific communication or transaction and the related user, client, or server application.

9-6.9 Remote Access Authentication

Postal Service information resources must support and maintain access control for personnel using networked, dial-in, and Internet connections to Postal Service information resources. Strong authentication or other stringent access controls must be implemented for personnel entering through dial-in, the Internet, or other non-Postal Service communication networks. Source restrictions (i.e., destination verification of remote session source address) may be used as a substitution to strong authentication for remote access.

9-6.10 Session Management

A computer session is a unique period of activity performed on or by an information resource usually associated with a login by a user. All information resources must implement session management standards specific for the information resource platform.

9-6.10.1 Session Establishment

Information resources must comply with session establishment requirements including, but not limited to, the following:

a. During a login, the information resource must allow the entire login sequence to be completed before providing any response to the initiator of the login.

b. The information resource must generate an alarm after an administrator-configurable number of consecutive incorrect login attempts across multiple accounts.

c. When the threshold for invalid consecutive attempts (normally six) for a given logon ID is reached, the information resource must deactivate access for the logon ID until a security administrator unlocks it.

d. Upon successful session establishment, the information resource must make available the date and time of the last successful login.

9-6.10.2 Session Expiration

Information resources must comply with session expiration requirements including, but not limited to, the following:

a. After the specified period of inactivity during the session (applicable standards defined by the manager, CISO ISS), the information resource must terminate the session and connection and require a successful re-authentication to regain access.

b. Following termination by the user or interruption by a power failure, system crash, or transmission problems, the session and connection must be dropped. The establishment of a new session requires the normal user identification, authentication, and authorization.

c. The information resource must provide an administrator-configurable session expiration (i.e., session lifetime). After the specified period of time, regardless of activity, the information resource must terminate the session, lock out the connection, and require a successful re-authentication to regain access.

9-6.10.3 Time-Out Requirements (Re-authentication)

The inactivity time-out standard for Postal Service information resources is a maximum of 30 minutes. After a maximum of 30 minutes of inactivity, the information resource must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password. Manual re-authentication must be required before access to the information resource is re-established. For remote access, the session must be terminated and the information resource disconnected from the network.

Note: Use the Postal Service standard or refer to the specific platform configuration standards for the applicable time-out requirements.

9-6.10.3.1 Workstations

The inactivity time-out standard for all Postal Service workstations is a maximum of 30 minutes. After a maximum of 30 minutes of inactivity, the time-out event must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password. Manual re-authentication must be required before access to the workstation is re-established.

9-6.10.3.2 Applications

The inactivity time-out standard for all application sessions must be set at a maximum of 30 minutes.

9-6.10.3.3 Remote Access

For remote access, the communications session is limited to 2 hours. After 2 hours, the workstation is disconnected from the network. The normal workstation inactivity time-out standard described above applies.

9-6.10.3.4 Failed Access Attempts

Failed access attempts and access attempts by unauthorized personnel or information resources must be rejected and recorded for audit trail and incident reporting purposes.

9-6.11 Authentication Requirements

All information resources must comply with authentication requirements including, but not limited to, the following:

a. The authentication process should protect the information resource from a replay attack.

b. During information resource recovery, authentication information must be recoverable without unauthorized disclosure or loss of data and information resource integrity.

c. The information resource must support a configuration capability that prevents authentication information (e.g., password, PIN number, token, or smart card) from being displayed in clear text or otherwise made available to any other user, including an administrator.

d. When the initial authenticator is created, the information resource must not divulge the authenticator to anyone other than the user and the authorized administrator.

e. The information resource should have the ability to authenticate itself to the user and to other software application components during the authentication sequence.

f. Where technically feasible, information resources must support process-to-process authentication.

g. Failed logon attempts must be recorded for audit trail and incident reporting purposes.

9-7 Confidentiality

Confidentiality is the security property that ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Information resources must have the capability to ensure that information is transmitted and stored in a way such that only authorized users are allowed access. Confidentiality is maintained through comprehensive and interrelated efforts that include, but are not limited to, the following:

a. Information designation.

b. Clearances and need to know.

c. Physical security.

d. Authentication of users.

e. Encryption.

9-7.1 Encryption

Encryption is the primary means for providing confidentiality services for information that can be stored or sent over the network, intranet, and Internet. Information resources that store or transmit sensitive-enhanced or sensitive information must have the capability to encrypt information.

9-7.1.1 Minimum Encryption Standards

The minimum encryption standard for the Postal Service is the Advanced Encryption Standard (AES) with a 128-bit encryption key. Triple Data Encryption Standard (DES) with 128-bit encryption key may be used if AES is not available for the information resource.

9-7.1.2 Required for Transmission and Storage on Removable Devices and Media

Information resources storing or processing sensitive-enhanced or sensitive information must implement approved encryption based on Postal Service encryption and key recovery policies. Encryption must be used for sensitive-enhanced and sensitive information that is transmitted or stored on removable devices or media. Encryption must be used for payment card industry (PCI) information throughout the life cycle. Encryption must also be used for sensitive-enhanced and sensitive information that is stored off Postal Service premises.

9-7.1.3 Recommended for Storage on Nonremovable Devices

Where technically feasible, encrypt sensitive-enhanced and sensitive information stored on nonremovable devices.

9-7.2 Use of Encryption Products

Encryption products must comply with requirements including, but not limited to, the following:

a. Information resources using encryption must use only algorithms and standard encryption products that are approved by the Postal Service and meet federal information processing standards and industry best practices.

b. All encryption products must support functionality of or integrate with applications to make encryption keys available to management. Any use of encryption without such technology must be approved in writing by the CISO.

9-7.3 Key Management

Key management is the generation, recording, transcription, distribution, installation, storage, changing, disposition, and control of cryptographic keys. Key management must be rigorous and disciplined because attacks against encryption keys are far more likely to occur and succeed than attacks against encryption algorithms.

9-7.3.1 Protecting Encryption Keys

Encryption keys must be treated as sensitive-enhanced information and access to those keys must be restricted on a need to know basis. The following principles apply to the protection and access of encryption keys:

a. If keying material is generated and stored, the information resource must provide secure key storage that is resistant to compromise through a logical or physical attack.

b. If hardware-based key generation and storage is used, the key must be stored in such a way that it cannot be retrieved in clear text.

9-7.3.2 Recommended Key Management Practices

The best way to mitigate the risk of keys being attacked is to store them in hardware on a secure physical device. Postal Service information resources should adhere to key management practices that include, but are not limited to, the following:

a. Generate strong keys.

b. Use split knowledge keys and establish dual control of keys.

c. Implement secure key distribution and storage.

d. Periodically change keys. Key management should be fully automated and not require manual steps.

e. Replace known or suspected compromised keys.

f. Revoke old or invalid keys.

g. Destroy old keys.

h. Generate and store all keys in hardware.

i. Never remove keys from the hardware and never store them in the host's memory.

j. Gain access to the hardware only through a trusted path.

k. Make sure key custodians sign a form stating they understand and accept their key-custodian responsibilities.

9-7.4 Key Management Requirements

Information resources must comply with key management requirements including, but not limited to, the following:

a. If the information resource supports key recovery, then access to the key must be restricted to authorized personnel.

b. The information resource must have the capability to enforce the immediate revocation of user accounts and the associated key(s).

c. Encryption keys must not appear in clear text outside a cryptographic device.

9-7.5 Elimination of Residual Data

The information resource must have the capability to ensure that there is no residual data exposed to unauthorized users.

9-8 Integrity

Integrity is the security property that ensures correct operation of information resources, consistency of data structures, and accuracy of stored information. Information resources must be installed and maintained in a manner that ensures the integrity of the information resources and their data.

Appropriate planning must occur before conducting security-related activities affecting the information resource in order to minimize the impact on the integrity of the information resource and on Postal Service operations (e.g., mission, functions, image, and reputation) and assets. Security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, testing, exercises, and retirement and disposal of hardware and media.

9-8.1 Information Resource Integrity

Information resource integrity ensures that information resources perform their intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Integrity provides assurance that under all conditions the operating hardware and software maintain logical correctness, reliability, and effective protection mechanisms. Acceptable integrity thresholds for processing and control devices in the MPE/MHE private nonroutable network address space are defined by Engineering.

Information resources must comply with information resource integrity requirements including, but not limited to, the following:

a. Security features designated in approved hardening standards must be invoked.

b. No information resource may undermine the integrity of underlying platforms or supporting infrastructure.

c. The information resource must perform integrity checks for system functions.

d. The information resource must retain the existing security parameters even after a restart or recovery.

e. Backup capability must be provided to restore the information resource to its former state.

f. Boundary checking must be implemented to prevent buffer overflow conditions.

g. The information resource must provide appropriate alert messages before executing potentially damaging commands.

h. The information resource must provide an administrator with the capability of retrieving the date and time associated with any security-related activity and the logon ID of the user who initiated the activity.

i. The information resource must provide mechanisms to detect duplicate authentic financial transactions.

j. The information resource must monitor the status of its components in real time to ensure that all components are still active and to prevent components from failing without detection.

9-8.2 Data Integrity Requirements

Data integrity is the security property that ensures that data meets a given expectation of quality and has not been exposed to accidental or malicious modification or destruction. Information resources must comply with data integrity requirements including, but not limited to, the following:

a. Information resources must have the capability to ensure that data is not modified, altered, or deleted without authorization in either storage or in transit.

b. Any unauthorized modification of data must yield an auditable security-related event.

c. The information resource must have the capability of identifying the originator of any information before that information is used in any restricted function of the information resource.

d. The information resource must log any attempt by the administrator to authorize any user to bypass the administrator-configured data integrity controls.

e. The information resource must protect data integrity by performing data integrity checks.

f. When data integrity checks fail, the information resource must reject the data.

9-8.3 Application Requirements

Management must be periodically notified about the accuracy, timeliness, and relevance of the information they use for decision making. Management must be notified if controls which ensure the integrity of information fail or if such controls are suspected of failing.

If information issued or released has been modified in any way, the recipients must be notified about the nature of the modification so that they can determine whether the modifications are significant enough to affect decision making. All incomplete or obsolete information must be suppressed and not distributed to users unless it is accompanied by an explanation which describes the status of the information.

Production data and software must be changed only by authorized people according to established written procedures. Production transactions must be properly authorized prior to updating production records whether these records are computer based or not.

To facilitate tracking and problem resolution, each accountable transaction must be time stamped, identified to person who submitted it, and assigned a unique sequence number or identifier. Line numbering must also be implemented for free-form text messages that deal with important business matters.

Sufficient controls must be implemented to ensure information is free from a significant risk of undetected alteration.

All rejected input transactions must be placed in a suspense file and listed in exception reports until such times as they are successfully resubmitted for processing or otherwise handled. All input transactions that are held in a suspense status pending further investigation must be either resubmitted or otherwise handled within 10 business days of original entry. Input transactions that are corrected for resubmission or that are suspended and later approved resubmission must be subjected to the same validation procedures (e.g., reasonable checks and formal edit checks) that original input transactions receive.

9-8.4 Management Requirements

Internal records must be periodically reviewed for reasonableness and accuracy. Reasonable checks include ratio analysis and accuracy checks include physical inventories. If records are discovered to be in error, they must be promptly corrected by authorized individuals using standard control procedures.

Important information on which management depends must be periodically compared with external sources or otherwise cross-validated to ensure that it is accurate.

9-8.5 End-User Computing Requirements

End-user computing, including spreadsheets and other user-developed programs, must be documented and regularly reviewed for processing integrity, including their ability to sort, summarize, and report accurately. For important reports, the logic should be reviewed periodically to ensure information is processed completely and accurately.

User-developed systems must be secured from unauthorized use. Audit logs must be periodically reviewed to detect unauthorized access attempts and take corrective action.

To facilitate audit trail requirements, transactions affecting sensitive-enhanced, sensitive, and critical information must be initiated only by receipt of source documents or computerized messages in which the originating individual and system are clearly identified. Proof of non-Postal Service sources can be achieved via digital signatures, message authentication codes (MACs), and encryption.

All end-user business-related representations must be truthful at all times.

9-9 Availability

Availability is the security property that ensures information resources are accessible by authorized personnel or information resources when required.

9-9.1 Capacity Planning and Scalability

For all information resources, capacity planning and scalability must be considered for both the information resources and network components, such as routers, firewalls, proxies, and encryption. Whenever technically feasible, consider scalable information resources that require little or no change to the configuration or the application when adding hardware or data storage.

9-9.2 Redundancy

Redundant systems for utilities, communications, mainframes, servers, and firewalls may be recommended where warranted to ensure the availability of critical information resources. The implementation of redundant systems should be based on a cost-benefit analysis and the recovery time objective (RTO). Infrastructure including telecommunication services must be engineered to not have a common point of failure.

9-9.3 Relationship of Criticality, Recovery Time Objective, and Recovery Point Objective

The criticality of an information resource is determined during the BIA, and the EIR is updated at the completion of the BIA process.

The RTO, which is the maximum allowable downtime for an information resource, is determined for information resource designated as critical. The RTO is the length of time it takes to restore the information resource. The RTO does not indicate how much data will be lost.

The RTO must be commensurate with the level of criticality. If there is a significant mismatch between the RTO and the criticality designation, the RTO and criticality designation must be reviewed. As a general rule the more critical the information resource, the lower the RTO. A lower RTO often requires a larger investment in BCM resources, which, in turn, results in higher costs. The RTO is determined in consultation with the DR service provider as the DR strategy is defined.

Also at this time, the data currency requirements/recovery point objective (RPO) is determined. The RPO indicates the maximum amount of allowable

data loss. It is the point in time (age) to which data must be recovered relative to the time of the disaster. It is the size of the window of opportunity for data loss. The amount of data loss is determined by backup methods and frequency of backup transport offsite.

9-9.4 Assuring Availability

Multiple technologies should be used to minimize the data loss and increase the availability of data for local and alternate site recovery. These technologies must provide for both traditional backup and recovery to meet local requirements in addition to the availability of data at the alternate processing site for disaster recovery. The movement of data for disaster recovery can be moved electronically over high-speed dedicated circuits via hardware data replication, remote tape vaulting, or information resource specific database replication/journaling technologies. The choice of technologies is dependent on the desired RPO and RTO.

9-9.4.1 Data Replication

Selection criteria: The files selected for data replication are determined by the placement of the data on the appropriate storage device that is configured for passive replication. Passive replication refers to a process when the data is changed and stored on the primary device and then the data is replicated to a device at the alternate site.

Frequency: The frequency of data replication should be aligned for minimal data loss and expected RPO for this service.

9-9.4.2 Remote Tape Vaulting

Selection criteria: The files selected for remote tape vaulting are determined by the usage of unique identifier(s) in the file name or specific request to the IT operations group. The supporting IT operations group needs to be contacted to receive the appropriate unique identifiers or to make specific site requests.

Frequency: The frequency of tape vaulting is dependent on the establish RPO for this service.

Inventory: An inventory of critical files that are remotely vaulted must be maintained. A copy of the inventory must be available at the alternate processing site to support business resumption process.

9-9.4.3 Application Database Replication and Journaling

The application owner who chooses to use a vendor-provided database replication and journaling services for high-availability services must procure the IT-approved product, then fund or perform the necessary configurations and reconfigurations.

9-9.4.4 Alternate Backup Requirements

All information resources not using one of the above technologies must implement secure backups. The information resource must have the capability to check the integrity of data read from a backup file when performing a restore function.

All essential components of an information resource required for continued operations must be backed up. The backup procedures must be documented. The responsible Postal Service manager must define the appropriate backup media and frequency.

Applications determined by the BIA as critical must implement backup and recovery strategies sufficient to meet the RTO and data currency requirements.

9-9.4.4.1 What to Back Up

Backups include, but are not limited to, operating systems, configuration files, general utilities, application software, data, supporting files and tables, scripts, standard operating procedures, specialized equipment, and related documentation.

9-9.4.4.2 When to Back Up

Back up software prior to migrating to test or production and prior to maintenance. Back up software after migrating to production and after maintenance. Back up information updated by batch processing at the successful completion of the update. Back up information updated by real-time processes at a frequency based on the RTO and RPO of the application.

9-9.4.4.3 Backup Schedules

All essential components must be backed up on a schedule that is sufficient to meet the RTO and RPO of the application or information resource as defined by the executive sponsor that controls the essential component and the CISO. Back-up job failures are properly documented, investigated, and remediated in a timely fashion.

9-9.4.4.4 Backup Inventory

An inventory of critical applications backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off site or in a fireproof container at the facility that hosts the application. An inventory of backup media and materials is recommended for all other information resources.

9-9.4.4.5 Backup Storage Requirements

Backup media must be stored in an environmentally controlled and secure location (e.g., a locked cabinet or room with controlled access). Backup media must be appropriately numbered, logged, and labeled as “Restricted Information”.

9-9.4.4.6 Off-Site Backup Storage Requirements

Backup media for critical criticality applications must be stored off site at a location that is not subject to the same threats as the original media. Off-site storage of backup media is recommended for all other information resources.

9-9.4.4.7 Backup Verification

Backup media for critical applications must be verified to ensure that backups are complete and can be read. From time to time, the application and associated backup hardware and software should be tested with the backup media to ensure the application can be successfully restored and

used. Verification of backup media is recommended for all other information resources.

Annually review the data backup policies and inspect the actual backup practices of third party providers.

9-9.4.4.8 Backup Disposal

All unneeded electronic backup media or hardware containing sensitive-enhanced or sensitive electronic media must be erased using a method that complies with the most current Postal Service policy and processes on the disposal of sensitive-enhanced and sensitive media.

9-9.5 Information Resource Recovery and Reconstitution

Critical information resources, including infrastructure and applications, must have the ability to be recovered and reconstituted to their original state following a disruption, failure, or disaster. This means all system parameters (either default or established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application software is reinstalled, information from the most recent backups is available, and the entire configuration has been fully and successfully tested at an alternate site. Authorization to request backup data is limited and restricted to approved Postal Service personnel.

Contingency plans must be developed and tested for critical infrastructure and telecommunication service providers and include recovery and reconstitution of critical applications. The EIR must be updated to identify which applications require the development and testing of continuity plans.

9-9.6 High Availability

High availability should be implemented where warranted, based on a cost-benefit analysis and RTO. Resources or processes that may be deployed to ensure high availability include, but are not limited to, the following:

a. Fault-tolerant information resources.
b. Redundant hard drives [e.g., randomly accessed independent disk (RAID) array], systems, and servers.
c. Uninterruptible power supplies (UPS), power conditioning systems, and backup generators.
d. Off-site vaulting of application transactions.
e. Disk mirroring of applications at site not subject to the same threats.
f. Hot-swappable components.
g. Secondary storage devices.
h. Continuous monitoring.
i. Automated fail-over and fail-back systems.

9-10 Security Administration

Security administration includes management constraints, operational procedures, and supplemental controls established to protect information resources. Sensitive-enhanced, sensitive, and critical information resources must implement logical access security.

9-10.1 Security Administration Requirements

Security administration functions that must be implemented for Postal Service information resources include, but are not limited to, the following:

a. Activating protective features (e.g., the login feature).

b. Displaying users logged on.

c. Creating, retrieving, updating, or deleting all security–related attributes of users, interfaces, and software and data elements.

d. Overriding or altering vendor-provided security defaults.

e. Configuring security-relevant options.

f. Configuring the display of security-related events.

g. Recording and archiving the information resource configurations.

h. Monitoring suspected activities related to a potential information security incident.

i. Detecting information security incidents promptly, isolating and investigating the problem, and recovering securely from the incident.

9-10.2 Security Administration Documentation Requirements

Security administrative requirements must be appropriately documented. These security administration documentation requirements include, but are not limited to, the following:

a. Cautions about functions and privileges that must be controlled when running a secure facility.

b. Administrator functions related to security, including adding or deleting users, changing user security characteristics, generating keying material, and revoking user-related security parameters.

c. Standards on consistent and effective use of security features, including their interaction and how to generate a new security configuration.

d. Standards for retaining accountability tracking information for an administrator-specified period of time.

e. Procedures necessary to start the information resource in a secure manner.

f. Procedures to resume secure operation after termination of information resource processes.

9-11 Audit Logging

All information resources must implement system-level audit logging. Audit logs include system logs, event logs, error logs, and Web logs.

Information resources must support audit log capabilities including, but not limited to, independently and selectively monitoring (in real time) the following:

a. The actions of any user currently logged on and automatic lockout of that user if necessary.

b. The activities at a specified terminal, port, or network address and automatic lockout of that input device if necessary.

9-11.1 Audit Logging Functionality Requirements

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred. Information resources must implement audit logging functions including, but not limited to, the following:

a. Providing adequate information for establishing audit trails relating to information security incidents (as part of forensics analysis) and user activity.

b. Supporting administrator-selectable alerts for specified security-related events.

c. Recording the logon ID or user ID accountable for the event.

d. Maintaining the confidentiality of authenticators (e.g., passwords) by excluding them from being recorded.

e. Maintaining the confidentiality of personally identifiable information (PII) and debit/cardholder data.

f. Protecting audit logs as sensitive information.

g. Protecting audit log control mechanisms from modification, deletion, or disabling of the function.

h. Restricting access to authorized users.

i. Generating real-time alarms indicating immediate attention is required for of operational problems (e.g., running out of storage space) and audit log malfunctions.

j. Providing authorized individuals with access to enable retrieval, printing, and archiving (copying to long-term storage devices) of audit log contents.

k. Providing administrators with audit analysis tools to selectively retrieve records from the audit log to produce reports.

l. Sanitizing audit log storage locations and media prior to reuse.

9-11.2 Audit Log Events

The logging of the following events must be considered for information resources:

a. All sessions established.
b. Invalid or unauthorized authentication attempts to access information resources.
c. Action of individuals with root or elevated privileges (e.g., system and database administrators).
d. Creation or changes in user or information resource security accounts, profiles, ACLs, privileges, and attributes.
e. Creation and deletion of system level objects.
f. Use of privileged accounts.
g. Shutdowns, restarts, and backups.
h. Installation and updates of software.
i. Access to audit logs.
j. Changes to logs.

The following security events must be captured at a minimum for each platform:

Mainframe ACF2:

a. Logon failures.
b. User account (i.e., LID) and group creation.
c. Assignment and modification of privileges.
d. Access and changes to Audit Log Reporting.
e. Access and changes to ACF2 rules.

UNIX:

a. Logon failures.
b. User logon and logoff.
c. -su and SUDO attempts.
d. Changes to system audit policy and configurations.
e. Changes to the file permissions and ownership of log files.

Windows Server and Windows Active Directory:

a. Windows account lockout (i.e., brute force attacks).
b. Windows audit log cleared (i.e., deletion of the Windows audit log).
c. Windows privileged activities by user (i.e., activities performed by privileged accounts).
d. Windows privileged user created (i.e., creation of a local system administrator).
e. Windows sensitive file access (i.e., access of sensitive/critical files).

IDMS:

a. Customer data changes.
b. Production updates to the dictionary objects (i.e., source code, maps, dialogues, and work records).

c. Creation/deletion/modification of dictionary privileges for a user.
d. Access and changes to audit logs.
e. Access and changes to system audit policy and configurations.

Oracle database:

a. Logon failures.
b. Metadata changes.
c. User account and group creation.
d. Assignment and modification of privileges.
e. Access and changes to audit logs.
f. Access and changes to system/application audit policy and configurations.

Teradata:

a. Logon failures.
b. User logon and logoff.
c. Metadata (e.g., table and schema) changes.
d. User account and group creation.
e. Assignment and modification of privileges.
f. Access and changes to Audit logs.
g. Access and changes to system/application audit policy and configurations.

DB2:

a. Logon failures.
b. Assignment and modification of privileges.
c. Access and changes to configuration baseline files.
d. Metadata (e.g., table and schema) changes.

9-11.3 Audit Log Contents

The information resource must record event information including, but not limited to, the following when available:

a. Date and time of the event.
b. Logon ID and MAC or IP address of the event initiator.
c. Event type and success or failure of the event if applicable.
d. Identification of information resources accessed.
e. Source host name and IP address generating the log event.
f. Destination host name and IP address generating the log event.
g. Transaction code or process ID.

9-11.4 Audit Log Protection

Secure audit logs so they cannot be altered, by:

a. Labeling audit logs as “RESTRICTED INFORMATION”.
b. Limiting the viewing of logs to those with job-related need (e.g., need to know and least privilege).

c. Protecting audit log files from unauthorized access, modifications, and destruction.

d. Promptly backing up audit log files to a centralized server or media that is difficult to alter.

e. Storing a backup copy of audit logs off site.

f. Using file integrity monitoring and change detection software on logs to ensure existing log data cannot be changed without generating alerts.

9-11.5 Audit Log Reviews

System administrators and database administrators must review audit logs regularly for potential security incidents and security breaches and maintain a record of the review. System administrators and database administrators must review audit logs regularly for potential security incidents and security breaches and maintain a record of the review. Any suspicious activity must be reported to management, investigated, documented and resolved in a timely manner. See 9-11.2, Audit Log Events, for details regarding the events that should be captured for each platform.

9-11.6 Audit Log Retention

Audit logs, whether in electronic or nonelectronic format, must be retained for 2 years, or in accordance with a legal hold, or as directed by the Postal Service Records Office (see Handbook AS-353, *Guide to Privacy, Freedom of Information Act, and Records Management)* and then destroyed in accordance with Postal Service policy.

This page intentionally left blank

10 Hardware and Software Security

10-1 Policy

Postal Service policy is to manage the procurement, configuration, operations, and maintenance of information resource hardware and software, whether located on Postal Service or non-Postal Service premises, in a manner that ensures information security. Hardware and software security must be implemented and maintained with the appropriate level of technical and administrative controls to protect the Postal Service technology and operations infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction. Chapter 10 addresses the following:

a. Hardware security.
b. Software and applications security.
c. General policies for hardware and software.
d. Configuration and change management.
e. Protection against viruses and malicious code.
f. Operating system, database management system, and application audit log requirements.

10-2 Hardware Security

Hardware security must be implemented based on Postal Service published standards on all computer hardware including, but not limited to, the following:

a. Mainframes.
b. Network devices.
c. Servers.
d. Workstations.
e. Portable devices.

10-2.1 Mainframes

Appropriate security controls must be enabled. For mainframe implementation of this security policy, contact the manager, Host Computing Services.

10-2.2 Network Devices

Appropriate security controls must be enabled on all network devices, including routers, hubs, and switches (see 11-3, Protecting the Network Infrastructure).

10-2.3 Servers

Postal Service servers must be protected commensurate with the level of sensitivity and criticality of the information and business function. Server installation and deployment must comply with standard configuration and deployment standards unique to the individual server platform. Implement only one primary function per server [e.g., a Web server, database server, and domain name server (DNS) should be implemented on separate servers). Configuration standards for servers in the mail processing and mail handling equipment (MPE/MHE) nonroutable address space environment are defined by Engineering.

10-2.3.1 Hardening Servers

All information resources must be implemented on servers hardened to Postal Service standards. Hardening standards must be implemented specific to each platform. These standards must delineate restricted and prohibited functions, port, protocols, and services. Hardening standards must be updated as new vulnerabilities are uncovered and updates are available.

Operating system and database software configurations, including services, protocols and functionality, must be reviewed on a periodic basis commensurate with the level of sensitivity and criticality of the information and business function. Operating system software configuration reviews are performed on a semi-annual basis for UNIX. Unnecessary services and protocols must be disabled. All unnecessary functionality such as scripts, drivers, features, subsystems, and file systems must be removed. Vendor supplied default passwords must be removed and common parameters must be set to prevent misuse or compromise.

Servers must not be deployed to a production environment prior to hardening. Servers must be updated when the server hardening standards are updated for that platform.

Note: The manager, Corporate Information Security Office (CISO) Information Systems Security (ISS), is responsible for the update and distribution of server hardening standards

10-2.3.2 Using Web Servers

All Postal Service Web servers, regardless of location, must use approved hardware and software with standard configurations to reduce likelihood of loss or compromise due to exploitation of configuration vulnerabilities. For Web or Internet projects under the direct control of the Postal Service, the development and testing must be conducted on specifically designated development Web servers. Web servers must not be implemented on individual workstations without prior written approval by the manager, CISO ISS.

10-2.3.3 Using Database Servers

Database servers must use security controls appropriate for the level of sensitivity and criticality of the information they contain. Database servers must be separate from other servers, including Web and application servers (see 10-2.3.4, Combined Web and Database Servers, for an exception).

Database servers located inside Postal Service firewalls must not be directly accessible from Web servers or other systems located outside firewalls. All database servers must be approved by the network connectivity review board (NCRB) prior to being deployed to the demilitarized zones.

Database servers must not be deployed to a production environment before hardening.

10-2.3.4 Combined Web and Database Servers

A Web server and database server may be placed on the same host if all the following requirements are met:

a. Application is not sensitive enhanced, sensitive, or critical.

b. Application is not Internet accessible.

c. Application is not on the DMZ.

d. Application is not enclaved with sensitive-enhanced, sensitive, or critical applications.

e. Application is operationally standalone, that is, does not interact with other database servers.

f. Host meets Postal Service server hardening standards.

10-2.4 Workstations

All workstations including desktops, laptop computers, notebook computers, palm tops, handheld devices, and wireless telephones must have appropriate security controls. Workstation installation and deployment must comply with standard configuration and deployment standards unique to that workstation platform. All personnel are responsible for protecting the information resources at their individual work location and abiding by all information security policies and procedures that apply to their individual environment.

All Postal Service desktops, laptops, and notebooks must have an approved personal firewall installed and personnel must connect to the Postal Service intranet at least once per week to receive the latest software patches, antivirus pattern recognition files, and personal firewall patterns. Appropriate configuration of the desktops, laptops, and notebooks to receive these patches and pattern updates is required. Personnel that fail to connect their desktops, laptops, and notebooks to the intranet in 30 days will be locked out and the user will need to call the IT Help Desk to be reinstated.

10-2.4.1 Physical Security

All Postal Service workstations must be protected, at a minimum, by secure physical access to the facility or room. Other physical security controls may include, but are not limited to: unique workstation identification (inventory control), identification card reader, screen protector or positioning screen to

restrict viewing from passersby, lockable keyboard, physical lock, and desk-fastening security equipment.

10-2.4.2 Password- or Token-Protected Screen Saver

Where feasible, all desktops, laptops, and notebooks must be configured at deployment to use password protected screen savers. After a period with no activity, password-protected screen savers will blank the screen; a password is then required to resume work. The maximum period of inactivity that initiates the screen saver must be 30 minutes or less as dictated by security needs. Users must protect the screen saver password just as they protect all other system passwords.

10-2.5 Portable Devices

Portable information resources must be protected against damage, unauthorized access, and theft. All personnel who use or have custody of portable devices, such as laptop computers, notebook computers, palm tops, handheld devices, wireless telephones, and removable storage media devices, are responsible for their safekeeping and the protection of any sensitive-enhanced, sensitive, and critical information stored on them.

All laptop and notebook computers must implement hard disk encryption. In addition, sensitive-enhanced and sensitive information on other portable devices must be protected (e.g., encrypted) when leaving a secure environment.

All Postal Service portable workstations such as laptop and notebook computers must have an approved personal firewall installed and connect to the Postal Service intranet at least once per week to receive the latest software patches, antivirus pattern recognition files, and personal firewall patterns. Appropriate configuration of the portable workstations to receive these patches and pattern updates is required. Portable workstations that fail to connect to the intranet in 30 days will be locked out and the user will need to call the IT Help Desk to be reinstated.

10-3 Software and Applications Security

Security attributes and capabilities must be selection criteria in the acquisition or development of all Postal Service software. The collection of features of the operating system, application, database management system, and utility software must be complementary and enhance the security of the system.

10-3.1 Software Safeguards

Software configuration and installation must include only the features and functions necessary to perform the required business activities. Controls must include, but are not limited to, the following:

a. Activating or enabling all safeguards embedded in computer software to restrict access to authorized users, maintain system performance, and to monitor for suspicious activity.

b. Document information security settings in the security plan.
c. Disabling or removing all features and files that have no demonstrable purpose.
d. Disabling or removing default privileged logon IDs, changing all default passwords, and removing guest accounts.
e. Removing test data.
f. Prohibiting use of administrative and root accounts for running production applications.
g. Limiting access to the specific files required.
h. Restricting access to systems software utilities to a limited number of authorized users on the basis of need-to-know.

10-3.2 Complying With Copyright and Licensing

All software used on Postal Service information resources must be procured in accordance with Postal Service policies and procedures and be licensed and registered in the name of the Postal Service. All personnel must abide by software copyright laws and must not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

10-3.3 Secure Transaction Compliance

10-3.3.1 Financial Requirements

Financial requirements must be implemented when processing e-Commerce financial transactions (Note: these requirements are set by the payment card industry).

10-3.3.2 Health Insurance Portability and Accountability Act Requirements

Health Insurance Portability and Accountability Act requirements must be implemented when processing health or medical information.

10-3.4 Version Control

All software that can be modified must be managed through the authorized Postal Service change control and management process (see 10-5, Configuration and Change Management). Software containing modifications, such as exits and supervisor calls, must be documented detailing the extent of the modifications. The modifications must be fully reviewed, tested, documented, and installed in a controlled environment to avert possible adverse effects on the security of the production environment.

10-3.4.1 Updating Software

Only authorized personnel may perform updates to the production application programs or operating system libraries/directories.

Individual access privileges must be approved by appropriate management officials.

After the system is changed, the security controls must be checked to ensure the security features are still functioning properly. Periodically (at

least annually) the security controls must be tested to ensure the information security controls are functioning as designed and documented.

Significant changes [as defined in the Certification and Accreditation (C&A) process] will cause the re-initiation of the C&A process.

10-3.4.2 Distributing Software

Controls must be in place to regulate and manage the distribution of Postal Service systemwide production applications to field sites. These controls must ensure that the correct version is installed on all nodes and that the code cannot be modified on the field computer systems.

10-3.4.3 Prohibited Software

Software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software must not be installed. All requests for software not on the infrastructure toolkit (ITK) must be directed to the Enterprise Architecture Committee (EAC) (see 10-4.2, Acquiring Hardware and Software).

10-3.4.4 Unapproved Software

Unapproved software is removed by the IT staff.

10-3.5 Operating Systems

All Postal Service information resources must use approved operating systems, including all approved updates and patches. Operating systems must have controls in place to prevent a compromise of the integrity of the computer operating system environment and must be configured to comply with operating system security requirements specified by Postal Service policies.

10-3.6 Application Software

Postal Service information resources must use only approved application software. Application software must be compatible with installed security software. Security activities for application software must be incorporated in the applicable life-cycle process during development. Application software developed in house or outsourced is subject to the C&A process.

10-3.7 Database Management Systems

All Postal Service information resources must use Postal Service-approved database management systems (DBMSs) that have been configured to comply with Postal Service security policies including:

a. Implement role-based access.

b. Authenticate all access by information resources, administrators, and users.

c. Prohibit direct SQL queries to the database.

d. Prohibit database servers located inside Postal Service firewalls from being directly accessible from Web servers or other information resources outside those firewalls.

10-3.7.1 DBMS Activity Journals

Each production DBMS must have a journal file to protect against accidental destruction of data or interruption in service. Journal files must be backed up as specified in the DBMS or the applicable business continuity plan.

10-3.7.2 DBMS Security Features and Views

All database tables must utilize the security features of the DBMS or equivalent (e.g., ACF2) to preserve the integrity of the database. Views and discretionary access controls must be used to protect sensitive-enhanced, sensitive, or critical information and enforce need to know.

10-3.8 COTS Software

Commercial-off-the-shelf (COTS) software must be acquired from a Postal Service-approved source. The EAC approves COTS software for use within the Postal computing environment. Requests for unapproved COTS software must be submitted to the EAC for review and approval.

Computer software purchased for the Postal Service must be registered to the Postal Service. COTS software used within the MPE/MHE nonroutable address space environment is approved by Engineering.

10-3.8.1 COTS Software Security Evaluation and Vulnerability Assessment

A COTS software security evaluation and vulnerability assessment must be performed for all proposed additions to the Postal computing environment. It is recommended that the COTS vulnerability assessment be periodically updated for COTS software associated with sensitive-enhanced, sensitive, and critical information resources.

10-3.8.2 COTS Independent Code Review

COTS applications that contain custom programming or scripts may be subject to an independent code review. The independent code review exams the custom source code and documentation to verify compliance with software design documentation, programming standards and to ensure the absence of malicious code. (See Handbook AS-805-A*, Information Resource Certification and Accreditation Process,* for the criteria for conducting an independent security code review.)

10-3.9 Browser Software

Workstations and applicable portable devices should use approved Postal Service standard browser software. All Web applications developed for Postal Service use must be compatible with the Postal Service standard browser software. The standard browser software must support encryption and comply with the privacy and cookie policies found at *www.usps.com.*

10-3.10 Third-Party Software

Third-party software is defined as follows:

a. Software developed for the Postal Service by a vendor, contractor, or other third party.

b. Other limited-distribution custom-built applications.

c. COTS software that has been modified with custom programming scripts or languages.

10-3.10.1 Ownership

Third-party software developed under contract or funded by the Postal Service must be considered the property of the Postal Service unless otherwise stated in the contract.

10-3.10.2 Licensing and Escrow of Custom-Built Applications

Third-party software not owned by the Postal Service but considered a required component of an information resource used in an essential business activity must be licensed to the Postal Service. The vendor of this software must periodically escrow the source code.

10-3.10.3 Assurance of Integrity

A written integrity statement must be provided with significant third-party software that provides assurances that the software does not contain undocumented features or hidden mechanisms that could be used to compromise the software or operating system security.

10-4 General Policies for Hardware and Software

10-4.1 Securing the Postal Service Computing Infrastructure

The Postal Service computing infrastructure must be protected through the implementation of information security standards, processes, and procedures.

Note: The manager, CISO ISS, is responsible for developing and maintaining an Enterprise Information Security Architecture and coordinating a secure Postal Service computing infrastructure by setting standards, and developing and/or approving the security processes and procedures.

10-4.2 Acquiring Hardware and Software

All hardware and software must be acquired from official Postal Service sources. Software not listed on the ITK must be approved by the EAC.

10-4.3 Using Approved Hardware and Software

All Postal Service information resources must use only hardware and software acquired from official Postal Service sources. All Postal Service information resources must use only software listed on the ITK. Software that is unlicensed, borrowed, downloaded from online services, public domain shareware/freeware, or unapproved personal software must not be installed. Personnel wishing to use information resources not on the ITK must obtain approval from the EAC.

Engineering must approve hardware and software used within the MPE/MHE environment.

10-4.4 Testing of Hardware and Software

Thorough testing of all new or modified hardware and software is required to ensure that there is no adverse effect on the security of Postal Service information resources.

10-4.5 Tracking Hardware and Software Vulnerabilities

Designated personnel in Customer Care Operations, Host Computing Services, Information Systems Security, and Engineering must be on hardware and software vendor advisory mailing lists and other forums appropriate to the information resources under their control. All vulnerability advisories involving hardware and software in use within the Postal Service computing environment must be documented and tracked.

10-4.6 Scanning Hardware and Software for Vulnerabilities

Scanning tools must have the ability to update the list of vulnerabilities to be scanned. Hardware platforms and software packages must be scanned on a regular basis. The scanning procedure must ensure adequate scan coverage and update the list of vulnerabilities.

10-4.7 Maintaining Inventories

All personnel are responsible for maintaining accurate inventories of Postal Service information resources assigned to them including hardware, software, firmware, and documentation. The inventory management process must ensure accountability and must include current copies of hardware and software maintenance agreements, licenses, purchase orders, and serial numbers.

10-4.8 Isolation of Postal Service Information

Postal Service data must not be commingled with non-Postal Service data.

10-4.9 Using Diagnostic Hardware and Software

Diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers) must be used only by authorized personnel for approved purposes (see 14-3, Monitoring).

10-4.10 Controlling Preventive and Regular Maintenance

Preventive and regular maintenance (and repairs) must be scheduled, documented, and controlled whether performed onsite or remotely. Information system components containing sensitive-enhanced or sensitive information must be sanitized prior to removal from a Postal Service facility. Maintenance records must be reviewed in accordance with manufacturer specifications and/or organizational requirements. Where possible

automated mechanisms are employed to schedule and conduct maintenance.

Preventive and regular maintenance must be performed only by authorized personnel. When maintenance personnel do not have the needed access authorizations, organizational personnel with appropriate access authorizations must supervise maintenance personnel during the performance of maintenance activities on the information system.

For critical information resources, service level agreements delineate the spare parts that must be maintained onsite for the repair of key information system components and the allowable time period for repair following a failure.

10-4.11 Controlling Maintenance Tools

Information system maintenance tools must be approved, controlled, and maintained on a regular basis. Automated mechanisms are employed, where possible, to restrict use of maintenance tools to authorized personnel.

Maintenance tools brought in to Postal Service facilities must be inspected by maintenance personnel for obvious improper modifications. Media containing diagnostic and test programs must be checked for malicious code prior to use.

All maintenance equipment capable of retaining sensitive-enhanced or sensitive information must be sanitized before it is removed from the Postal Service facility. If the equipment can not be sanitized, it must remain in the Postal Service facility or be destroyed.

10-5 Configuration and Change Management

The Postal Service configuration and change management process applies to all Postal Service information resources regardless of where the information resource is hosted or managed. Security-related requirements for the following areas are presented in 8-2.4, Configuration and Change Management:

a. Configuration component inventory.
b. Standard hardened configurations.
c. Change/version control.
d. Patch management.
e. Security testing of the configuration.

10-5.1 Significant Changes

Significant changes to sensitive-enhanced, sensitive, and critical information resources require the re-initiation of the C&A process.

10-5.1.1 Computing Platform

A significant change to an information resource (hardware and software) is determined by the extent of the change and the impact on the protection

features. Any change to the information resource that adversely affects security controls is considered a significant change.

10-5.1.2 Application

A significant change to an application system is determined by the impact of the change on the input, processing, or output associated with the application. Any change to the application system that adversely affects security controls is considered a significant change.

10-6 Protection Against Viruses and Malicious Code

All Postal Service information resources must be protected against the introduction of viruses and other types of malicious code that can jeopardize information security by contaminating, damaging, or destroying information resources. Malicious code includes harmful and other unwanted code such as viruses, worms, keystroke loggers, botnets, Trojans, trap doors, time bombs, activity trackers, remote control agents, snoopware, spyware, and adware.

10-6.1 Virus Protection Software

10-6.1.1 Installation

All information resources within the Postal Service must have active virus protection software installed and enabled. Unauthorized personnel must not modify the configuration of virus protection software.

10-6.1.2 Scanning

To ensure Postal Service perimeter security, Information Security Services conducts scans for malicious code on the firewalls, FTP servers, mail servers, intranet servers, Internet application protocols, and other information resources as necessary.

10-6.1.3 Updating

Centralization of automatic updates to virus software is critical to updating information resources with the latest version of virus detection software and updated files of virus types (signature files). The managers, computing operations/infrastructures, are responsible for ensuring that virus protection software and signature files are current and distributed to Postal Service information resources. Virus protection software and signature files must be periodically updated or immediately updated whenever a new threat is perceived.

10-6.2 Other Protection Measures

10-6.2.1 Protecting Shared and Retrieved Files

All personnel must run virus protection software prior to using shared or retrieved files from workstations, laptops, removable media, and other information resources.

10-6.2.2 Evaluating Active Content or CGI Code

A code review must be conducted on sensitive-enhanced, sensitive, or critical information resources that contain active content code or CGI scripts (see 8-5.5.3, Conduct Code Review). In addition to the code review, information resources that contain active content code or CGI scripts may be subject to an independent code review (see 8-5.5.7, Conduct Independent Code Review).

10-6.2.3 Protecting Applications

All application software and supporting files must be protected such that an error will be generated if there is an unauthorized attempt to modify the software. All activities involving modification of software must be logged.

10-6.2.4 Creating Backups before Installation

To assist with the post-virus restoration of normal computer activities, all computer software must be copied prior to its initial usage, and such copies must be stored in a secure location. These copies must not be used for ordinary business activities but must be reserved for recovery from computer virus infections, hard-disk crashes, and other computer problems.

10-6.2.5 Checking for Viruses Before Distribution

All software, information, or any other type of digital media must be tested to identify the presence of computer viruses and other malicious code prior to distributing to Postal Service organizations, personnel, businesses, or the public.

10-6.2.6 Spyware Protection Measures

All information resources within the Postal Service must be protected against the introduction of spyware. A layered-defense must be implemented combining antispyware software with anti-virus software, a personal firewall, host anomaly detection/intrusion prevention software, spam and content filtering for inbound e-mail, pop-up blocker protection, and user education. Unauthorized personnel must not modify the configuration of spyware protection software.

10-6.2.7 Automated Mechanisms

Information resources must provide automated mechanisms to support the handling of information security incidents.

10-7 Operating System, Database Management System, and Application Audit Log Requirements

Operating system, database management system, and application audit logs must be sufficient in detail to facilitate reconstruction of security-related events if a compromise or malfunction is suspected or has occurred. For events where immediate attention is required, the audit Audit logs must be reviewed periodically for potential security incidents and security breaches.

The audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified. (See 9-11, Audit Logging, for additional requirements.)

10-7.1 Operating System Audit Logs

Operating system audit logs must record security-related events. Operating systems must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of operating system integrity. Operating system software must have the capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction.

10-7.2 Database Management System Audit Logs

Database management systems must implement appropriate logging of security-related events.

10-7.3 Application Audit Logs

Sensitive-enhanced, sensitive, and critical applications that have logging capability must implement appropriate logging of security-related events.

This page intentionally left blank

11 Network Security

11-1 Policy

The Postal Service network infrastructure must be protected at a level commensurate with its value to the Postal Service. Such protection must include the implementation of the physical, administrative, and technical security controls and processes that safeguard the confidentiality, availability, and integrity of the network and the data in transit in accordance with Postal Service policies and procedures.

Network controls and processes are necessary to do the following:

a. Safeguard data traffic.

b. Detect and prevent unauthorized access.

c. Respond to computer security incidents.

d. Detect and correct transmission line errors.

e. Ensure message integrity throughout the system.

f. Provide network and data security.

g. Ensure that recovery procedures are in place and working.

h. Specify the appropriate auditing procedures.

This policy applies to all information resources, technologies, services, and communications that are part of the Postal Service network, including the following:

a. All transmission technologies used on behalf of the Postal Service in Postal Service or non-Postal Service facilities [(e.g., local area networks (LANs); wide area networks (WANs); voice communications; videoconferencing systems; voice messaging systems; desktop video communications; satellite broadcasts; facsimile transmission; and all other transmissions over landline, wireless, or Internet-based networks].

b. All types of information and network services, data, voice, image, and multimedia communications, regardless of transmission technology.

The Postal Service prohibits the attachment of any nonapproved network device, to include routers, switches, repeaters, wireless access-points, and firewalls to any point of the network. Direct questions about whether a network device is approved to the NCRB via e-mail to *ncrb@usps.gov*. The Postal Service removes or disables nonapproved network devices added to the network infrastructure.

11-1.1 Network Architecture

Network architectures — the appearance, functions, locations, and resources used in the network infrastructure — must be designed with the appropriate level of administrative and technical security controls, including network addresses, network services and protocols, network perimeters, and network integrity controls.

11-1.2 Network Infrastructure

The network infrastructure — facilities, equipment, services, protocols, and applications used to transmit, store, and process information — must be protected through the following requirements:

a. Physical security.
b. Network asset control.
c. Network configuration information.
d. Identification and authentication.
e. Authorization.
f. Hardening standards.
g. Secure enclaves.
h. Network isolation.
i. Vulnerability scans, penetration testing, and vulnerability assessments.
j. Firewalls.
k. Demilitarized zones.
l. Network traffic monitoring.
m. Network connection.
n. Business partner and third party.
o. Remote access.
p. Network audit logs.
q. Wireless networks.

11-1.3 Wireless Network Security

Wireless technology, including wireless local area networks (WLANs), cellular technologies, radio frequency identifier (RFID) tag applications, Bluetooth technologies, and personal area networks (PANs), must be approved by the network connectivity review board (NCRB) before procurement and integration.

11-2 Network Architecture

The network architecture must be designed with the appropriate level of administrative and technical security controls, including the following:

a. Network addresses.
b. Network services and protocols.

c. Network perimeters.

d. Network integrity controls.

11-2.1 Network Addresses

All network names and addresses must be managed and approved by the central addressing authority within telecommunications services (TS). Internal network addresses must be protected, and access to internal network addresses is based upon a need to know and least privilege. When appropriate, TS conceals network addresses and provides translation of nonroutable addresses.

11-2.2 Network Services and Protocols

All information resources must use only network services and protocols approved by the NCRB. All nonapproved protocols and services must be disabled at the perimeter. Minimum requirements for extending the Postal Service intranet into the remote site are as follows:

a. Secure NCRB approval.

b. All connections to any network(s) other than the intranet must be controlled by firewalls managed by Postal Service TS or a TS designee.

c. Network changes to the agreed upon configuration must be approved by TS.

d. TS or a TS designee must have unrestricted physical access to the network.

e. All equipment connected to the network must meet current Postal Service security hardening standards.

f. Connections to the Postal Service intranet must be firewalled in a manner similar to current Postal Service secure enclave firewalling.

g. Business partner connections, including those that are an extension of the Postal Service intranet, must be Postal Service-managed via firewall or other network filtering device.

h. Passwords used to manage systems on the network must not be used to manage other systems or networks.

i. All remote site systems administrators must have a Postal Service security clearance.

11-2.3 Network Perimeters

Perimeters are clearly defined boundaries that must be established to securely control the traffic between Postal Service information resources and all other networks. All inbound or outbound network traffic must pass through appropriate access control devices, such as firewalls, before reaching Postal Service information resources. The manager, TS, must ensure perimeter monitoring and may block the Internet Protocol (IP) address of a computer performing hostile reconnaissance or attacks against Postal Service networks. Other appropriate defensive measures to protect the Postal Service information resources may be used, as approved by the manager, TS and/or the manager, CISO ISS.

Note: The Office of the Inspector General (OIG) manages, secures, monitors, scans, and supports its own network and information technology (IT) infrastructure. The OIG network connectivity to the Postal Service intranet must comply with the requirements and processes for approved connectivity to the Postal Service intranet.

11-2.4 Network Integrity Controls

The manager, TS, establishes a system of controls to safeguard the data traffic, detect and correct transmission line errors, ensure message integrity throughout the system, and protect computers and other telecommunications endpoints. Adequate audit procedures must be employed to monitor and analyze network integrity.

11-3 Protecting the Network Infrastructure

The network infrastructure consists of the facilities, equipment, services, protocols, and applications used to transmit, store, and process information. The Postal Service network infrastructure is protected through the following:

a. Ensuring physical security.
b. Maintaining network asset control.
c. Protecting network configuration information.
d. Implementing identification and authentication.
e. Implementing authorization.
f. Implementing hardening standards.
g. Determining when a secure enclave is required.
h. Establishing secure enclaves.
i. Isolating the Postal Service networks.
j. Conducting vulnerability scans, penetration testing, and intrusion detection.

11-3.1 Ensuring Physical Security

Servers and other components of the Postal Service networks must be located in areas secured to a level commensurate with the sensitivity and criticality of the information stored, processed, or transmitted. Access to network infrastructure components must be limited to authorized personnel.

11-3.2 Maintaining Network Asset Control

All infrastructure components must be inventoried at regular intervals and labeled for asset management and physical protection.

11-3.3 Protecting Network Configuration Information

Network information, including, but not limited to, configurations, addresses, subnet masks, secure enclave locations, and firewalls must be protected and

treated as sensitive. Access to network configuration information must be based upon the security principles of need to know and least privilege.

11-3.4 Implementing Identification and Authentication

Personnel must be required to identify and authenticate themselves to the network before being allowed to perform any other actions on the network.

11-3.5 Implementing Authorization

Access to information resources must be granted based on the job function, appropriate clearance, need to know, separation of duties, and least privilege.

11-3.6 Implementing Hardening Standards

Information resources supported by networking must be hardened to meet or exceed the requirements documented in Postal Service hardening standards specific to each platform. Hardening refers to the process of implementing additional software and hardware security controls.

Note: The manager, CISO ISS, is responsible for the distribution of information resource hardening standards.

11-3.7 Determining When a Secure Enclave Is Required

Enclaves can be implemented to enforce separate security zones (e.g., to segregate information resources with similar issues and risks). An enclave is a virtual LAN configured to isolate a subnet/host system from other systems based on risks. All traffic in and out of the enclave is forced through a control interface.

Enclaves are required for the following information resources:

a. Information resources accessible from the Internet (i.e., externally facing information resources).

b. Information resources remotely managed by Postal Service business partners.

c. Controlled enhanced, controlled, or critical information resources where the risks warrant additional protection. Information resources designated as controlled enhanced, controlled, or critical must be assessed by the manager, CISO ISS, to determine if the resource should reside in a secure enclave. A completed business impact assessment (BIA) and the architectural diagram must be submitted to the manager, CISO ISS, for review and determination of whether additional enclave protection is required.

11-3.8 Establishing Secure Enclaves

Secure enclaves are network areas where special protections and access controls, such as firewalls and routers, are utilized to secure information resources. Secure enclaves apply security rules consistently and protect

multiple systems across application boundaries. Secure enclaves must be implemented as follows:

a. Employ protection for the highest level of information sensitivity in that enclave.

b. Reside on network segments (subnets) separate from the remainder of Postal Service networks.

c. Use “network guardians,” such as packet filtering or application proxy firewalls, to mediate and control traffic.

d. Set enclave server rules and operational characteristics that can be enforced and audited.

e. Allow only predefined, securable information traffic flows.

f. Restrict administration to a small, well-defined set of system administrators.

g. Employ intrusion detection systems and intrusion prevention systems.

h. Audit the network boundary controls through the performance of network scanning procedures on a regular basis.

i. Restrict sharing of physical devices for virtual machines among multiple enclaves.

11-3.9 Isolating Postal Service Networks

Postal Service networks must be isolated from non-Postal Service networks (e.g., business partner and vendor networks). Postal Service and non-Postal Service network devices must not be commingled. Nonpublicly available Postal Service information must be isolated from non-Postal Service information (e.g., business partner and vendor information) in transit.

11-3.10 Conducting Vulnerability Scans, Penetration Tests, and Vulnerability Assessments

Only personnel authorized by the CISO are permitted to conduct scanning, penetration testing, and vulnerability scans and assessments of Postal Service information resources. During audits and investigations, the OIG may conduct scanning, penetration testing, and vulnerability assessments as deemed appropriate. The OIG has the authority to scan and conduct penetration testing and vulnerability assessments on their own network and IT infrastructure.

11-3.10.1 Vulnerability Scans

Requests for vulnerability scans must be directed to the manager, CISO ISS, for approval. Vulnerability scans are conducted on Postal Service information resources by CISO ISS or their designee.

11-3.10.2 Intrusion Detection

Requests for intrusion detection must be directed to the manager, CISO ISS, for approval. Intrusion detection is conducted for Postal Service networks by CISO ISS or their designee. The OIG conducts intrusion detection at its discretion.

11-3.10.3 Penetration Testing

Requests for penetration testing must be directed to the manager, CISO ISS, for approval. Penetration testing is conducted for Postal Service networks by the CISO ISS or its designee. The OIG conducts penetration testing on Postal Service networks at its discretion.

11-4 Internet Technologies

The Postal Service uses Internet technologies in the following environments:

a. Internet.

b. Intranet.

c. Extranet.

11-4.1 Internet

Access to the Internet from Postal Service information resources must be routed through Postal Service-approved access control technology (e.g., firewalls and proxies).

11-4.2 Intranet

An intranet is a network based on Internet technologies located within an organization's network perimeter. The Postal Service operates and maintains an intranet for the conduct of Postal Service business. Access control technology, such as firewalls and filtering routers, must be used to protect the Postal Service intranet at the network perimeter to provide access control and support for auditing and logging.

11-4.3 Extranet

An extranet is a network based on Internet technologies that allows an organization to conduct business and share information among business partners, vendors, and customers. Business partners must comply with the requirements and process of the NCRB contained in the Handbook AS-805-D, *Information Security Network Connectivity Process*. Business partners must be limited in their access to the specific information resources identified in the network connectivity request that is approved by the NCRB.

11-5 Protecting the Network/Internet Perimeter

The perimeter between the Postal Service network and the Internet environments must be protected through the following:

a. Implementing Internet security requirements.

b. Implementing firewalls.

c. Establishing demilitarized zones (DMZs).

d. Monitoring network traffic.

11-5.1 Implementing Internet Security Requirements

Internet-accessible information resources, such as those residing on DMZs, must implement security requirements that include, but are not limited to, the following:

a. Securely partitioning each Internet-accessible environment (e.g., the intranet and extranet) from each other.

b. Using firewalls or filtering devices to screen and monitor incoming and outgoing traffic.

c. Supporting encryption to protect the storage and transmission of sensitive-enhanced and sensitive information.

d. Performing continual evaluation, testing, monitoring, and maintenance of the firewalls.

e. Applying real-time monitoring, auditing, and alerting to detect intrusion, fraud, abuse, or misuse.

Access control technology, such as firewalls and filtering routers, must be used to protect the Postal Service intranet at the network perimeter to provide access control and support for auditing and logging.

11-5.2 Implementing Firewalls

A firewall is a safeguard or type of gateway that is used to control access to information resources. A firewall can control access between separate networks, between network segments, or between a single computer and a network. A current-generation firewall is generally not a single component but a strategy composed of both hardware and software for protecting an organization's resources.

Direct public access between the Internet and the Postal Service intranet must be controlled by a firewall. A firewall must be installed at each Internet connection and between any DMZ and the Postal Service intranet.

Secure NCRB approval in advance of establishing network connectivity to an information resource involving firewall changes.

11-5.2.1 Firewall Configurations

Postal Service firewalls must be configured to do the following:

a. Deny all services not expressly permitted (i.e., deny all inbound and outbound traffic not specifically allowed).

b. Restrict inbound Internet traffic to Internet Protocol (IP) address with the DMZ (ingress filters).

c. Prevent internal addresses from the Internet into the DMZ.

d. Implement dynamic packet filtering (i.e., only allow "established" connections into the network).

e. Secure and synchronize router configuration files (i.e., running configuration files and start-up configuration files used to reboot machines must have the same secure configuration).

f. Audit and monitor all services to detect intrusions or misuse.

g. Notify the firewall administrator and system administrator in near real time of any item that may need immediate attention.

h. Run on a dedicated computer.

i. Stop passing packets if the logging function becomes disabled.

j. Disable or delete all nonessential firewall-related software, such as compilers, editors, and communications software.

11-5.2.2 Firewall Administrators

Each firewall or logical group of firewalls must have adequate resources assigned for firewall administration. Firewall administrators are responsible for ensuring compliance with standards for configuration and approved services and protocols.

11-5.2.3 Firewall Administration

All Postal Service firewalls must be located in a controlled environment. Firewall configuration standards must include a description of roles and responsibilities for management of all components.

Firewall administration must be performed from the local console or via remote access if approved by the manager, CISO ISS, and appropriately secured through strong authentication and encryption. Firewall configurations must be protected and treated as sensitive. Access to firewall configuration information must be based upon the security principles of need to know and least privilege.

11-5.2.4 Firewall System Integrity

Firewall rule sets must be reviewed every 6 months. Firewall system configuration and integrity must be validated and tested periodically by the firewall administrator.

11-5.2.5 Firewall Backup

The firewall (e.g., system software, configuration data, and database files) must be backed up as determined in the appropriate business continuity plan.

11-5.3 Establishing Demilitarized Zones

DMZs are network segments between intranets, extranets, and the Internet that provide increased security for data transfer between information resources, vendors, and the public. DMZ requirements include the following:

a. Web servers and electronic commerce systems accessible to the public must reside within a DMZ with approved access control implemented via a firewall or gateway.

b. Sensitive-enhanced, sensitive, and critical information must not reside within a DMZ.

c. All inbound traffic to the intranet from the DMZ must be passed through a proxy-capable device.

d. Virtualization is not allowed in the DMZ.

11-5.4 Monitoring Network Traffic

The Postal Service network perimeter must be monitored for network connectivity, services, and traffic. Monitoring must be conducted on both active and inactive connections.

11-6 Network Connections

11-6.1 Establishing Network Connections

The NCRB must approve in advance the establishment of network connectivity. Any connectivity to the Postal Service network must allow monitoring.

11-6.2 Requesting Connections

The NCRB provides the mechanism for requesting, reviewing, evaluating, and approving connectivity between non-Postal Service individuals and organizations wishing to establish connectivity to the Postal Service intranet.

11-6.3 Approving Connections

Requests for connectivity to the Postal Service intranet must be reviewed, evaluated, and approved by the NCRB. All requests for connectivity must follow and comply with the requirements identified in the NCRB request process described in Handbook AS-805-D.

11-7 Business Partner Connectivity Requirements

Business partner (or contractor) connectivity must be requested and funded by a Postal Service sponsor.

Connections using either existing BP ISP connectivity or frame relay service directly connected to the Postal Enterprise are protected by firewalls and security processes that restrict business partners to the IP address or addresses, server or servers, and ports or protocols they are explicitly authorized to access.

Business partners must be limited in their access to the specific information resources identified in the network connectivity request that is approved by the NCRB. No business partner is ever granted “open access” to Postal Service computing resources.

To protect the integrity of the Postal computing environment, business partners must have written information security policies describing how they will protect their proposed connection to the Postal Service and must include a copy of these security policies with their NCRB request.

Business partners must comply with the requirements and process of the NCRB contained in the Network Connectivity Process [link] including, but not limited to, the following:

a. Initiating requests with the executive sponsor for access to the Postal Service intranet.
b. Complying with all Postal Service information security policies.
c. Allowing site reviews by the Inspection Service or CISO.
d. Allowing audits by the OIG.
e. Reporting any security incident immediately to the CIRT and executive sponsor.
f. Notifying the executive sponsor when connectivity is no longer required.

11-8 Limiting Third-Party Network Services

Network services approved for third-party connectivity must be governed by the principle of least privilege and limited to those services and devices needed to perform the business function requested. The default must be to deny all access except those services specifically approved by the NCRB.

When establishing third-party connections, access controls and administrative procedures must be implemented to protect the confidentiality of Postal Service information resources. The third party must be responsible for protecting its private network infrastructure and information and must not rely on the Postal Service to perform this function.

11-9 Remote Access Requirements

Remote access privileges are restricted to authorized personnel and must be approved by appropriate management through eAccess before being granted. Remote workstations and laptops must be physically secured to prevent unauthorized access to the device and the Postal Service intranet. The use of personal information resources to remotely connect to the Postal Service intranet must be approved and connectivity must be managed through an approved virtual private network (VPN) solution.

11-9.1 Authentication

Information resources should be capable of strong authentication on application or network connections requiring remote access. Remote access requires users or devices to authenticate at the perimeter or connect through a firewall. Remote user communications must occur through encrypted VPN channels.

11-9.2 Virtual Private Network

A VPN provides end users with a way to securely access information on the Postal Service intranet over an untrusted network infrastructure or an untrusted public network such as the Internet. Postal Service VPN requirements include, but are not limited to, the following:

a. Any Postal Service VPN solution must provide end-to-end encryption and strong authentication capability.

b. Employees must submit an electronic request for computer access, or its equivalent, to obtain access to Postal Service information resources through a VPN.

c. Business partners requiring access to Postal Service information resources through a VPN must submit a formal request to the NCRB in accordance with the Information Security Network Connectivity Process.

d. Any VPN solution used for business partner connectivity must be capable of filtering access to specific information resources, and the connection must allow monitoring.

e. Any computing device connecting to the Postal Service intranet through a VPN must implement an approved personal firewall configured to Postal Service standards, as defined by CISO ISS

f. The end user has the responsibility to gain access and fund the Internet Service Provider (ISP) service when accessing Postal Service resources. The Postal Service does not provide recommendations for any local ISP access. Once a communication path to the Internet through the ISP has been established, the VPN session is initialized through the Internet to the Postal Service network.

11-9.3 Modem Access

Modem access for all information resources to and from Postal Service networks must be approved in writing in advance by the manager, CISO ISS, and must implement the information resource protection measures described below.

Note: Additional modem approval by the manager, CISO ISS, is not required for approved remote access services (e.g., VPN or point-to-point protocol (PPP).

Any workstation on the Postal Service intranet with approved modem access must:

a. Implement an approved personal firewall configured to Postal Service standards as defined by CISO ISS.

b. Disconnect from the Postal Service intranet prior to establishing alternate or additional connections to any network such as the Internet.

c. Initiate protection measures to ensure that the system has been cleaned of any malicious code prior to being permitted to connect to the Postal Service infrastructure.

d. Deactivate modem immediately after use.

11-9.4 Dial-in Access

All dial-in access to and from Postal Service networks must be approved in advance by the responsible Postal Service manager and implemented by the manager, TS. All approved dial-in access must be established through Postal Service centralized dial-in services.

11-9.5 Telecommuting

Personnel working at alternative work sites must only use Postal Service approved computer hardware, software, and virus protection software when working on Postal Service business, when sharing files with the Postal Service, or when communicating through phone lines or the Internet with the Postal Service. Any approved personal hardware must have the latest security patches installed, Postal Service-approved virus software installed with the latest pattern recognition file, and, if connecting via the Internet, a Postal Service-approved personal firewall must be implemented.

11-9.6 Remote Management and Maintenance

To protect the integrity of the Postal computing environment, use of remote administration and maintenance software and associated security controls must be approved by the manager, CISO ISS, in cooperation with the requesting organization.

Remote management and maintenance must be controlled and activity logs maintained. The remote access links, frequency of access, and associated controls must be documented in the security plan for the information resource. Two-factor authentication must be implemented and all communications must be encrypted. When remote management and maintenance is completed, the remote access connection must be disconnected and disconnection verified.

Organizations performing remote access must implement the same general level of security as the system being accessed. Instances of remote management and maintenance must be audited on a regular basis.

11-10 Network Audit Log Requirements

Networks including firewalls and controlled interfaces must have an audit capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction. Network audit logs must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of network integrity. Network audit logs must be sufficient in detail to facilitate reconstruction of security-related events if a compromise or malfunction is suspected or has occurred. For events where immediate attention is required, the audit utility must trigger alarms that are directed to the proper location for action.

Network audit logs must be reviewed periodically for potential security incidents and security breaches. Audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified. (See 9-11, Audit Logging, for additional requirements.)

11-11 Wireless Networking Requirements

Wireless devices and the supporting network infrastructure are subject to the following wireless security requirements and standards:

a. Wireless baseline requirements.

b. Wireless solutions.

c. Standard wireless solution.

d. Process for requesting nonstandard wireless solutions.

e. Bluetooth and personal area network applications.

f. Wireless LAN device management.

g. Compliance and monitoring requirements.

Note: This policy does not cover wireless devices (e.g., cellular phones, pagers, and radio systems) unless they transmit data (see MI AS-860-2003-2, Data Stewardship: Data Sharing Roles and Responsibilities).

11-11.1 Wireless Baseline Requirements

The following baseline requirements are key to ensuring basic functionality, maximum bandwidth, and appropriate network security:

a. Wireless applications must be capable of “mutual” device and user authentication (i.e., the device, the user, and the network must recognize each to be who they say they are).

b. There must be a secure link between a device and an access point (AP).

c. The installation of access points, wireless cards, or any wireless technology must be approved in advance by the NCRB because of the risks such installations can introduce to the Postal Service intranet, networks, and all connected information resources.

d. Wireless and wired networks must be developed and maintained separately and distinctly. A firewall is required between the wired and wireless network segments if Postal Service certificates are not used to authenticate the devices to the network.

Connecting APs or using wireless technology without proper prior approval introduces an unacceptable risk to the Postal Service intranet and other assets. Nonapproved wireless technology must be removed from the Postal Service computing environment.

11-11.2 Wireless Solutions

Wireless technologies enable one or more devices to communicate without physical connections — without requiring network or peripheral cabling. Wireless technologies use the radio frequency spectrum to transmit data and such technologies present security-related challenges. Wireless solutions are grouped as follows:

a. Standard wireless solution.

b. Nonstandard wireless solution.

Devices that meet the current WLAN standard solution do not require a firewall between wireless devices and wired networks. All other devices require a firewall between wireless devices and wired networks.

11-11.3 Standard Wireless Solution

11-11.3.1 General Requirements

This standard technology solution is predicated on the implementation of the following general requirements:

a. Assurance that the device is a member of the USA domain.

b. Assurance that it is a Postal Service-managed device using approved virus protection, security patches, and personal firewalls.

c. Authentication of the user through Active Directory (AD) credentials.

d. Mutual authentication of device/client and remote authentication dial-in user service (RADIUS) server through Postal Service internal Certification authority (CA) machine certificates.

11-11.3.2 Architecture Requirements

Technical requirements for standard wireless architecture solutions are:

a. The standard architecture for WLAN authentication/encryption must be an ACE device capable of using:

(1) A Postal Service Internal CA machine certificate authenticating to AD.

(2) Temporal key integrity protocol (TKIP) encryption.

(3) WiFi protected access2 (WPA2) for key management (WPA only if WPA2 is not available).

(4) Protected extensible authentication protocol (PEAP) authentication.

b. Users must authenticate to AD and be authorized for wireless access.

c. Users and devices must be registered members of AD.

d. Users must be able to authenticate using AD credentials.

e. Devices such as workstations must be able to mutually authenticate to a RADIUS server using Postal Service Internal CA certificates.

f. The technology solution must use a Microsoft supplicant client and the device must be ACE Windows XP compatible.

g. Clients must be able to download, store, and use a Postal Service internal CA machine certificate.

h. Clients must be able to support WPA2 and TKIP.

i. Protocols (e.g., PEAP) capable of supporting Microsoft machine certificates must be used.

j. Workstation/wireless card clients must be AD group policy object configurable.

k. Drivers and cards must be compatible with Postal Service standards and certified by TS for use within the Postal Service network.

l. Service set identifier (SSID) standardization must be implemented to support mobility.

11-11.3.3 How to Request Standard Wireless Services

Standard wireless connectivity is requested as follows:

a. Wireless connectivity must be requested via e-mail to *NCRB@email.usps.gov* or through the NCRB Web page on the IT Web site.

b. Wireless infrastructure must be requested through TS.

c. Wireless cards/client devices must be purchased via the ADEPT II contract accessible via *http:///it,* Resource Toolbox, Online Applications.

d. User wireless services must be requested via eAccess at *https:// eacess.*

11-11.4 Process for Requesting Nonstandard Wireless Solutions

The following process must be followed for business solutions including the use of wireless technology that do not meet the standards previously defined:

a. Obtain NCRB approval to proceed.Before pursuing a nonstandard wireless technology solution, approval to proceed from the NCRB must be obtained. The NCRB requires a business case for the alternate solution. The NCRB dictates the non-negotiable standards that the alternate solution must be compliant with.

b. Develop an architecture design. Develop an engineering architectural design in conjunction with TS. TS should validate compliance and functionality of the design to ensure that it will not adversely affect the current Postal Service solutions.

c. Obtain NCRB approval of the architectural design.

(1) Obtain approval of the application, the engineering architecture, and all wireless devices from the NCRB.

(a) For implementations involving MPE/MHE, contact the responsible design engineering organization that will send an e-mail to *NCRB@email.usps.gov* or submit a request through the NCRB Web site. The design engineering organization may also present the MPE/MHE project to the NCRB.

(b) For other implementations, contact the IT portfolio manager who will send an e-mail to *NCRB@email.usps.gov* or submit a request through the NCRB Web page on the IT Web. The portfolio manager will also act as a presenter to the NCRB on the requestor's behalf.

(2) At a minimum, the NCRB will evaluate against the following criteria prior to approval for implementation of wireless technology:

(a) Proper naming with regards to SSID.

(b) SSID broadcast turned off.

(c) Encryption of data between a device and an access point, or an ancillary downstream device. The majority of wireless APs have some inherent encryption capabilities.

(d) Trust between wireless devices. When setting up APs, there should be appropriate authentication — particularly a mutual authentication mechanism between a wireless device and an access point (802.11x) and user-based authentication when applicable (i.e., token, username/password).

(e) Appropriate logging/intrusion detection on the wireless segment, either on the access point or related device.

(f) The requirement for whether a firewall is needed between the wireless AP and WAN.

(g) Centralized, secure administration using unique user name and passwords that are compliant with Postal Service policy. Ideally, all wireless user accounts should be located in a common repository.

(h) Firewall and virus protection implementation on devices.

(i) Request through eAccess if Postal Service Internal CA machine certificates are required.

(j) Devices are remotely manageable by TS.

d. d.Obtain a wireless site survey. A wireless site survey must be performed to obtain maximum benefit of the wireless devices and to maintain appropriate security. TS arranges for the site survey via the Postal Service intranet contract. Normal turn-around time is 62 days; expedited is 30 days. The survey results will place the APs, offer channel sections, and specify other physical and programming parameters.

e. e.Acquire, program, and install device. After NCRB approval and review of the site survey report, the wireless infrastructure devices may be purchased by the customer through TS, who will then configure the devices. When the devices are programmed, they are sent to the site ready to be installed by the Postal Service intranet vendor.

11-11.5 Bluetooth and Personal Area Network Applications

Bluetooth and personal area networks (PANs) require approval from the NCRB prior to deployment.

All implementations of Bluetooth and PAN must meet the requirements for a nonstandard wireless solution and the following requirements:

a. Radio frequency range must be managed, using only the minimum signal required, to perform the task and periodically check for confinement.

b. Device pair bonding (mutual authentication) must be used. Ensure the Bluetooth bonding environment is secure from eavesdroppers. If the authenticator (e.g., PIN, password, and shared secret) meets Postal Service aging and storage requirements, the standard password criteria apply (see 9-6.1, Passwords), otherwise the authenticator must be complex and a minimum of 16 characters.

c. The link between devices must be encrypted during the authentication exchange process and also when sensitive-enhanced or sensitive information is transmitted. Use security mode 3.

d. Bluetooth or PAN configuration files must be periodically checked to ensure the security policy is enabled on devices where the files are accessible by end users.

11-11.6 Wireless LAN Device Management

TS or its designee remotely manage all devices that connect to the network using 802.11x technology, that incorporate TACACS, and have RADIUS authentication. Periodic software updates and product enhancements are downloaded to APs as required to improve performance and enhance security. Access point management also includes constant operating assessments of the device. Any malfunctions or loss of effectiveness generate an alert for resolution.

11-11.7 Procurement Requirements

When procuring wireless hardware, software, and services, consider the requirements stated in items a through s below in order to comply with the Postal Service wireless security policy. For any particular wireless application, all of the requirements may not apply. The security requirements should be included in procurement documents to adequately protect the wireless application and reduce the residual risk to an acceptable level.

Wireless devices should be capable of supporting the following requirements:

a. For devices intended for stationary deployment (e.g., in vehicles or on loading docks), capable of being solidly secured (e.g., to the vehicle or building). This requirement also applies to add-on modules.

b. Capable of requiring a “power-on” password prior to the device operating. This password is in addition to the specific user authentication password.

c. Capable of ensuring device authentication and strong (at least two-factor) user authentication. The wireless device must have the capability to be configured to query a secondary device for access when the primary server is offline.

d. Be WiFi protected access (WPA) certified. Has built-in security features, including data link-level encryption, 802.1x-compliant authentication model, and regular rotation of encryption keys.

e. Contain secure authorization software/firmware.

f. Where extensible authentication protocol (EAP) is used, capable of proper password management (e.g., aging and complexity criteria). The wireless device must have the capability to support password changes in a pre-established timeframe.

g. Capable of ensuring that users can be securely authenticated when operating locally or remotely. The device automatically senses when it is operating in a connected manner and uses the proper authentication.

h. Capable of implementing mutual authentication between the device and an access point.

i. Capable of being Active Directory-compliant for authentication purposes. Exceptions must be documented.

j. Capable of logging events.

k. Contain cryptography to attain the desired levels of integrity, authentication, and confidentiality. The Postal Service's minimum standard is 128-bit AES (Advanced Encryption Standard). When AES is not available for the wireless device, then 128-bit triple DES (Data Encryption Standard) may be used.

l. Capable of providing a secure channel for access point administration.

m. Capable of supporting end-to-end cryptographic protection for transmitting sensitive-enhanced and sensitive information where the traffic traverses network segments other than the wireless segment.

n. Capable of dynamic encryption key rotation. The wireless device must have the capability to support rotation of encryption keys in a pre-established timeframe.

o. Capable of supporting a timeout mechanism that automatically prompts the user for a password after a period of inactivity. The period of inactivity must be configurable via the device set-up procedure and ignore the keep-alive process (pings or loop socket-to-socket packets) for automated programs.

p. Capable of deactivating all communication ports and network associations during periods of inactivity.

q. Capable of implementing a personal firewall on wireless clients.

r. Capable of supporting static IP addresses and dynamic host configuration protocol (DHCP) on remote wireless equipment.

s. Capable of shielding authentication credentials against interception through short interval "authentication tunnels" (i.e., TLS standard).

Technical support for the integration of the wireless devices into the Postal Service infrastructure with other technological initiatives must be scoped, planned, and available in a timely and accurate manner (e.g., remote access for MPI, structured wiring switches, and SEF access).

11-11.8 Deployment Requirements

It is imperative to carefully plan the deployment of wireless technology. It is much more difficult to address security once deployment and implementation have occurred; therefore, security should be considered from the initial planning stage through deployment and operation.

Fulfilling the requirements stated in 11-11.8 will ensure compliance with the Postal Service wireless security policy. For any particular wireless application, all of the requirements may not apply. The information systems security officer (ISSO) must work with the executive sponsor to select the security requirements that must be implemented to adequately protect that application and reduce the residual risk to an acceptable level.

11-11.8.1 Administrative Security Requirements

Administrative security controls and management practices are crucial to operating and maintaining a secure wireless network. Wireless administrative security requirements are:

a. Do not install access points, wireless cards, or wireless devices to gain access to the Postal Service intranet without prior written approval from the NCRB.

b. Submit a detailed Security Plan to the NCRB along with the request for wireless connectivity.

c. Implement configuration/change control to ensure that equipment (e.g., access points) has the latest software release that includes security feature enhancements and patches for discovered vulnerabilities.

d. Review security-related mailing lists for the latest security vulnerabilities and alerts and respond accordingly.

e. Test software patches and upgrades.

f. Install security patches in a timely manner.

g. Use approved standardized configurations that reflect the information security policy and hardening standards to ensure consistency of operation.

h. Change system defaults that come with the wireless access points, including SSID, password, read/write community strings, and IP addresses set by the manufacturer.

i. Implement firewalls between access points and the wired network.

j. Conduct periodic scans to identify unauthorized access points and other devices that can disrupt the wireless network or compromise the security of the Postal Service intranet.

k. Disable wireless devices not included in the authorized wireless inventory.

l. Conduct information security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies (including the fact that robust cryptography is essential to protect the "radio" channel, and that theft of equipment is a concern).

m. Ensure that users know where to report lost or stolen wireless devices.

n. Perform a risk assessment to understand the value of the assets that need protection and document the residual risk following the application of all security countermeasures in the wireless deployment.

o. Centralize wireless security administration and actively monitor user connections.

p. Turn off communication ports and network associations during periods of inactivity when possible.

q. Perform perimeter surveys to review and adjust radio transmit power settings to prevent spillover (i.e., the leakage of Postal Service wireless radio signals beyond the perimeter of Postal Service property).

r. Use nonintelligible SSID identifiers, cryptographic keys, and administrative passwords.

s. Access point information fields must not be populated with Postal Service-identifiable information.

t. Bridging must always be disabled on access points and on remote wireless equipment that also has wired connectivity.

u. Disable SSID broadcasts on all wireless equipment.

v. Minimize broadcasts from access points or broadcasts on a segment (e.g., access point connected to a wired hub), and limit access point associations.

w. Ensure no microwave ovens or cordless phones are within sufficient range to create interference on WLANs.

x. Install antivirus software and malicious and unauthorized content inspection monitors on portable wireless devices.

y. Ensure access control lists clearly identify application rights (authentication) for all wireless users.

z. Avoid placing sensitive-enhanced or sensitive information on a handheld device. Store sensitive-enhanced or sensitive information encrypted and delete it from the handheld device when no longer needed.

aa. Synchronize mobile wireless devices with the corresponding workstations regularly.

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

11-11.8.2 Physical Securhity Requirements

Physical security controls should be implemented to mitigate some of the risks such as theft of equipment and insertion of rogue access points, including wireless network monitoring devices. Physical security controls

(e.g., barriers, access control systems, and guards) are the first line of defense. Wireless physical security requirements are as follows:

a. Deploy physical access controls (e.g., photo ID, card badge readers) to the building and other secure areas to protect against tampering and theft.

b. Solidly fix devices not under continuous user control (e.g., left in vehicles or on loading docks) to the vehicle or building through the use of physical locks and cables to minimize the risk of loss or theft.

c. Stow handheld devices in locked rooms and cabinets especially when left unattended for long periods (e.g., overnight).

d. Secure add-on modules to minimize the risk of loss or theft, since they sometimes are as much of a target as the primary handheld device.

e. Ensure access points are physically secure from tampering.

f. Locate authentication servers in protected areas behind access points.

g. Where sensitive-enhanced or sensitive information is transmitted, ensure external boundary protection (e.g., a fence or locked doors) is in place around the perimeter of the building or buildings.

11-11.8.3 Technical Security Requirements

Technical security controls should be implemented to mitigate risks such as eavesdropping, traffic analysis, masquerading, replay, message modification, and denial of service. Wireless technical security requirements are as follows:

a. Implement a “power-on” password based on Postal Service standards for each mobile wireless handheld device.

b. Implement appropriate password management (e.g., aging) for all handheld devices.

c. Implement mutual authentication between a wireless device and an access point.

d. Implement authentication for users whether operating locally or remotely (i.e., authenticate to the device or to the network).

e. Provide only specific services (e.g., HTTP, HTTPS, and SMTP).

f. Control access between the WLAN and wired LAN with a firewall.

g. Implement timeout mechanisms that automatically prompt the user for a password after a period of device inactivity.

h. Implement nonrepudiation access check for financial transactions.

i. Use the wireless access point for access only.

j. Configure the wireless access point properly.

k. Set wireless access points at 1, 6, and 11 so they do not compete and interfere with each other. If a nonstandard channel is used, it will indicate a possible “man-in-the-middle” attack.

l. Routinely test the inherent security features (e.g., authentication and encryption) that exist in wireless algorithms to protect sensitive-enhanced and sensitive information.

m. Encrypt data between a device and an access point, or ancillary downstream device utilizing Postal Service encryption standards (e.g., implement wired equivalency protocol using a 104/128-bit key).

n. Use a VPN to secure communication between WLAN and LAN resources.

o. Implement mandatory access control (MAC) address filtering.

p. Use a HTTP/SHTTP proxy to access the Internet.

q. Turn off ad hoc networking and ensure your wireless network interface card (NIC) remains in “infrastructure only” mode.

r. Use temporal key integrity protocol (TKIP) to provide data encryption including a pre-packet key mixing function, a message integrity check (MIC), an extended initialization vector with sequencing rules, and a rekeying mechanism.

s. Implement 802.1x and EAP to provide a framework for strong user authentication.

t. Employ Postal Service standard end-to-end cryptographic protection to transmit sensitive-enhanced and sensitive information over other network segments, including wired segments or the Internet.

u. Even when approved cryptography is used, employ additional countermeasures (e.g., strategically locating access points, firewall filtering, blocking, and installation of antivirus software) as required.

v. Employ automated key rotation.

w. Install personal firewall software on all mobile networked wireless devices.

x. Implement appropriate logging and intrusion detection where any wireless equipment is used.

11-11.8.4 Maintenance Security Requirements

Maintaining a secure wireless network and associated devices requires significant effort, resources, and vigilance. Wireless maintenance security requirements are as follows:

a. Maintain a full topology of the wireless network.

b. Label and keep inventories of the fielded wireless and handheld devices including MAC addresses and serial numbers.

c. Create frequent backups of data on mobile wireless equipment.

d. Perform periodic security testing and vulnerability assessment of the wireless network.

e. Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.

f. Apply patches and security enhancements in a timely manner.

g. Vigilantly monitor wireless technology for new threats and vulnerabilities.

h. Install the latest antivirus software on mobile wireless equipment.

i. Implement a secure channel for access point administration.

j. Configure alerts to data volume, packet collisions, and retries.

k. Conduct site surveys and adjust radio transmit power settings to avoid transmissions beyond Postal Service-owned property.

l. When disposing of handheld devices that will no longer be used, sanitize memory to prevent the disclosure of sensitive-enhanced or sensitive information and clear configuration settings to prevent the disclosure of restricted network information. Where portable hard drives are used, sanitize the disk in accordance with this handbook.

11-11.8.5 Security Requirements for Using a Public Hot Spot

Personnel connecting to public WLANs in airports, hotels, restaurants and such must take the following precautions:

a. Turn off file and print sharing from your wireless device.

b. Clear your list of “preferred networks.”

c. Turn off ad hoc networking and ensure your wireless card remains in “infrastructure only” mode.

d. When using a virtual private network to connect back to the Postal Service Intranet, disable split tunneling.

e. Use a personal firewall that detects malicious scanning of your wireless device.

11-11.9 Compliance and Monitoring Requirements

Security assessments and audits are essential tools for checking the security posture of a wireless technology and for determining corrective action to ensure the network remains secure. It is important to perform regular audits using wireless diagnostic hardware and software. Administrators should periodically check for rogue access points and against other unauthorized access.

Only authorized personnel may use diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers).

12 Business Continuity Management

12-1 Policy

In accordance with Federal Continuity Directive 1 (FCD 1) "Federal Executive Branch National Continuity Program and Requirements" dated February 2008, the Postal Service must develop, implement, test, exercise, and maintain a Business Continuity Management (BCM) program that provides management direction during the time an incident or a disaster occurs that affects the computing infrastructure, personnel, or facility of a major information technology (IT) site in order to protect its personnel and assets and to reduce the likelihood and impact of a disruption to essential business functions for both itself and its customers. All functional organizations and personnel must adhere to the business continuity management plans and strategies outlined in the BCM program plan and Headquarters' Continuity of Operations (COOP) plan.

This policy applies to all major information technology (IT) sites, and Accounting Service Centers (ASCs), the Shared Service Centers (Finance and Human Resources), the Material Distribution Center (MDC), and all organizations that use or support information resources in the United States Postal Service.

12-2 Business Continuity Management Program

BCM is a holistic management process that identifies potential impacts that threatens an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interest of the organization's key stakeholders, reputation, brand, and value-creating activities. BCM must be owned and fully integrated into the organization as an embedded management process. (Source: Business Continuity Institute.)

BCM is a management process that encompasses the following:

a. Resides within each organization and involves the protection of essential assets and continuity of business operations and services as a major responsibility to our customers, business partners, and employees.

b. Develops and maintains policies and procedures to support the resumption of critical, time-sensitive business processes, including critical business information systems and essential business functions, in the event of their disruption.

c. Includes the organization's strategic and tactical plans; policy and procedures; risk and opportunities related to regulatory agencies; industry organizations; suppliers; business processes; and the business units, people, information resources, functions, activities, and facilities.

d. Integrates all disciplines from human and information resources, facility and security management to, crisis communications and public relations, business processes, functions, and information systems.

BCM is a single approach that joins the following major recovery services:

a. **Business Recovery** focuses on the business processes and procedures to ensure a comprehensive strategy that minimizes the risk and cost in case of a disruption of information technology service.

b. **Disaster Recovery** directs and guides appropriate actions for the recovery of essential information technology business functions and activities to ensure an orderly recovery from a wide range of potential emergencies or threats that affect the computing infrastructure.

c. **Crisis Management** ensures communications systems are in place to notify first responders, to keep employees informed, and to update business partners and clients.

d. **Emergency Response** provides evacuation procedures that identify type of evacuation, assembly points, and head-count activities.

Together, the services provide guidance to Postal Service organizations responsible for mission assurance functions to manage the recovery process during and after an incident.

12-3 BCM Objectives

BCM objectives include the following:

a. Preparing personnel for potential emergencies by periodically testing and updating all business continuity plans.

b. Limiting the number of decisions that must be made following a significant service interruption (those that cause a portion of a facility to be disabled).

c. Eliminating the need to develop new procedures during the recovery process.

d. Minimizing the recovery time to restore critical applications and core business processes and functions.

e. Increasing organizational credibility with customers, business partners, and stakeholders by formalizing documentation processes to ensure availability and accuracy of the information for stakeholders.

f. Supporting and enhancing compliance with Sarbanes-Oxley requirements and federal standards (e.g., NHSPD 20/21, FISMA 2002, and NIST 800-53).

g. Fostering business relationships with the Postal Service enterprise through better IT organizational understanding of the business.

h. Positive marketing of BCM capabilities. (Effective BCM allows the Postal Service to provide high-service levels and thus win business.)

12-4 Headquarters Continuity of Operations Plan

The Headquarters' (HQs) Continuity of Operations (COOP) Plan is a deliberate and preplanned movement of selected key principals and supporting staff to a relocation facility.

The plan defines the essential functions and activation and relocation procedures for HQs' personnel during an incident. The essential functions are prioritized and include the organizational role and responsibility of each office. The essential functions are used as the primary business processes to be recovered should an incident occur at the HQs' building. The COOP also provides input into the business impact analysis strategy to use to determine recovery priorities should an incident occur at one of the major IT sites.

This page intentionally left blank

13 Security Incident Management

13-1 Policy

Postal Service information resources must be protected against events that may jeopardize information security by contaminating, damaging, or destroying information resources. The Postal Service requires that all information security incidents be immediately reported to the Computer Incident Response Team (CIRT) regardless of whether damage appears to have been incurred.

Security incident management topics addressed in this chapter include the following:

a. Information security incident identification.

b. Incident prevention, reporting, and containment.

c. CIRT incident process and activities.

All personnel must adhere to the incident prevention, reporting, and containment standards to ensure adequate protection of Postal Service information resources.

13-2 Information Security Incident Identification

Information security incidents are events, whether suspected or proven, deliberate or inadvertent, that threaten the integrity, availability, or confidentiality of information resources. The reporting of incidents enables the responsible organizations to review the security controls and procedures; establish additional, appropriate corrective measures, if required; and reduce the likelihood of recurrence. To protect the Postal Service computing environment, the manager, Corporate Information Security Office (CISO), may become involved at any point on any level for information security-related incidents impacting the Postal Service.

Reortable incidents include, but are not limited to, the following:

a. Physical loss, theft, or unauthorized destruction of Postal Service information resources (e.g., missing or damaged hardware, software, or electronic media).

b. Unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information.

c. Internal or external unauthorized access attempts to access information or the facility where the information resides.

d. Unauthorized activity or transmissions using Postal Service information resources.

e. Internal or external intrusions or interference with Postal Service networks (e.g., denial-of-service attacks, unauthorized activity on restricted systems, unauthorized modification or deletion of files, or unauthorized attempts to control information resources).

f. Information resources with system software that is not patched to the current level.

g. Information resources with virus protection software that is not patched to the current level or is disabled.

h. Information resources with virus pattern recognition files that are not current.

i. Sudden unavailability of files or data normally accessible.

j. Unexpected processes (e.g., e-mail transmissions that start without user input).

k. Files being modified when no changes in the files should have occurred.

l. Files appearing, disappearing, or undergoing significant and unexpected changes in size.

m. Systems displaying strange messages or mislabeled files or directories.

n. Systems becoming slow, unstable, or inaccessible (e.g., will not boot properly).

o. Data altered or destroyed or access denied outside of normal business procedures.

p. Detection of unauthorized personnel in controlled information security areas.

q. Security violation, suspicious actions, or suspicion or occurrence of embezzlement or other fraudulent activities.

r. Suspected bribery, kickbacks, and conflicts of interest.

s. Revenue loss involving an information system.

t. Prohibited mass electronic mailings.

u. Potentially dangerous activities or conditions.

v. Illegal activities.

w. Violation of Postal Service information security policies and procedures.

x. Identity theft.

13-3 Incident Prevention, Reporting, and Containment

13-3.1 Incident Prevention

The following actions by Postal Service personnel can help prevent information security incidents:

a. Display proper badge when in any Postal Service facility.

b. Be aware of your physical surroundings, including weaknesses in physical security and the presence of any unauthorized visitor.

c. Use only approved computer hardware and software with the latest patches installed.

d. Use updated virus protection software and pattern recognition files.

e. Do not download, install, or run a program unless you know it to be authored by a person or company that you trust.

f. Use a personal firewall.

g. Use a strong password of at least eight characters composed of upper- and lower-case alphabetic, numeric, and special characters.

h. Encrypt sensitive-enhanced and sensitive information physically removed from a Postal Service facility.

i. Encrypt sensitive-enhanced and sensitive information in transit.

j. Back up data stored on local workstation and physically secure the backup copies.

k. Be wary of unexpected attachments. Know the source of the attachment before opening it. Remember that many viruses originate from a familiar e-mail address.

l. Be wary of URLs in e-mail or instant messages. A common social engineering technique known as phishing uses misleading URLs to entice users to visit malicious Web sites. URLs can link to malicious content that, in some cases, may be executed without your intervention.

m. Be wary of social engineering attempts to solicit sensitive-enhanced or sensitive information (e.g., account numbers and passwords).

n. Users of technology such as instant messaging and file-sharing services should be careful of following links or running software sent by other users.

13-3.2 Incident Reporting

Information security incidents must be immediately reported to the CIRT via telephone at 1-866-USPS-CIR(T) or 1-866-877-7247 or via an e-mail to *uspscirt@usps.gov.* The CIRT telephone number is a 24 X 7 hotline. Do not dismiss a suspected incident or discount its seriousness.

In addition to the CIRT, the following personnel may be notified, as appropriate:

a. Help Desk at 1-800-USPS-HELP or 1-800-877-7435.

b. Immediate supervisor or manager.

c. Local system administrator or local technical support.

d. Security control officer (SCO).

e. Inspection Service at 1-877-876-2455.

f. Office of the Inspector General (OIG) at 1-888-877-7644.

A PS Form 1360, *Information Security Incident Report,* must be completed and submitted to the CIRT. An acceptable facsimile with the same information required on the form may be submitted.

13-3.3 Incident Containment

When an information security-related situation or incident is suspected or discovered, personnel must take steps, as directed by the CIRT, to protect the information resource(s) at risk. Appropriate actions are the following:

a. Do not shut down or power off a system after a computer incident occurs.

b. Do not make any changes to the equipment or network in question without direction from the CIRT.

c. Do not discuss or e-mail anyone about the situation or incident unless directed to do so by the CIRT.

d. Follow CIRT instructions with regard to options and strategies for containment and recovery from the incident.

e. Close and lock doors to protect unattended equipment.

f. Turn off computer monitor so screen cannot be viewed.

g. Challenge personnel without badges.

Supervisors or managers who suspect, discover, or are notified of a security-related event must initiate the following response procedures to contain the incident, protect the confidentiality and integrity of Postal Service information, and ensure business continuity:

a. Notify the CIRT for assistance to contain, eradicate, and recover from the security incident.

b. Notify the Inspection Service of a physical security incident.

c. Document in a journal or log all conversations and actions taken during the incident handling and response process and make this log available to management personnel on request.

d. Ensure personnel follow contingency plans for recovering from disruptive incidents.

e. Ensure the completion of a PS Form 1360.

13-4 CIRT Incident Process and Activities

13-4.1 Preliminary CIRT Activities

The following preliminary activities can improve the CIRT's ability to respond to information security incidents:

a. Develop an incident response plan. Predetermine necessary actions and responses to specific classes of incidents to facilitate making decisions under pressure with minimal information.

b. Implement secure connections to make intrusion detection system (IDS) policy changes and attack signature updates.

c. Verify automated responses from IDS.

d. Conduct penetration testing at times known only to personnel with a need to know.

e. Regularly review available information sources (e.g., advisories and research findings) to maintain currency.

f. Notify management of potentially harmful events.

g. Prioritize the severity of information security incidents.

h. Document lessons learned to improve CIRT operations.

13-4.2 CIRT Incident Process

13-4.2.1 Incident Categorization

Incidents must be categorized based on severity and associated response times. The severity of the incident will determine the appropriate notification process and escalation procedure. Incident severity levels and response times are defined as follows (per the Postal Service CIRT severity code procedures):

a. Severity 1 — National Impact: Incidents with the greatest negative impact on the Postal Service. Severity level 1 is assigned when an incident has national impact or when multiple systems or sites are down or seriously affected. Response timeframe: within 4 hours.

b. Severity 2— Site Impact: Incidents impacting a major IT or field site or local area network (LAN) segment. Response timeframe: within 24 hours.

c. Severity 3 — Customer Impact: Incidents impacting one or more workstations, employees, contractors, or customers. Response timeframe: within 3 business days.

d. Severity 4 — Minimal Impact: Incidents with minimal or no impact. Response timeframe: within 10 business days.

13-4.2.2 Processing Incidents Reports

The CIRT is responsible for the following:

a. Categorizing incidents.

b. Protecting the confidentiality of information contained in the incident report and subsequent information identified in the analysis.

c. Ensuring legal issues, requirements, and restraints caused by criminal and civil investigations are appropriated addressed.

d. Logging and tracking security incident reports.

e. Monitoring incidents to ensure appropriate response and timely resolution of security incidents.

f. Engaging appropriate organizational resources (e.g., virus response team, OIG, and Inspection Service).

g. Evaluating and escalating incident reports requiring further action.

h. Retaining incident reports, supporting evidence, and journals for 1 year or for a time period determined by the OIG.

i. Providing Inspection Service and OIG access to all reported information security incidents.

j. Complying with federal sector security incident reporting requirements.

13-4.2.3 Incident Investigation

A member of the OIG-CCU team is co-resident with the CIRT and investigates, along with the Inspection Service, violations of state and federal laws enacted to protect the authenticity, privacy, integrity, and availability of electronically stored and transmitted information.

13-4.2.4 Incident Analysis

The CIRT analyzes security incidents and prepares reports summarizing the causes, frequency, and damage assessments of information security incidents.

CIRT management analyzes the CIRT reports to improve the information security program and keep Postal Service executive management apprised on the state of information security.

13-4.2.5 Incident Escalation

It may be necessary to escalate an individual incident up the management chain based on the following criteria:

a. Number of sites and systems under attack.

b. Type of data at risk.

c. Severity of the attack.

d. State of the attack.

e. Source or target of the attack.

f. Impact on the integrity of the infrastructure or cost of recovery.

g. Attack on a seemingly “secure” information resource.

h. Personnel awareness of the attack.

i. New attack method use.

13-4.2.6 Incident Closure

Before an incident is closed the incident must be categorized; the root cause must be determined; damage must be assessed and reported to management and one or more of the national CIRTs if required; and the incident’s closure confirmed with the initiator.

14 Security Compliance and Monitoring

14-1 Policy

All Postal Service information resources are the property of the Postal Service. The Postal Service has the legal right to monitor and audit the use of its information resources as necessary for compliance with policies, processes, procedures, and standards to ensure the appropriate use and protection of Postal Service information resources.

The activities of all Postal Service personnel who use Postal Service computing resources may be subject to audit or monitoring, and any detected misuse of Postal Service computing resources may be subject to disciplinary action up to and including removal, termination, and criminal prosecution.

Security topics addressed in this chapter include the following:

a. Compliance.

b. Monitoring.

c. Audits.

d. Confiscation and removal of information resources.

This monitoring policy does not apply to Postal Service customers who visit the Postal Service Web site (i.e., no attempt is made to identify individual customers or their usage habits). See the Postal Service Internet Privacy Policy Statement for additional information.

14-2 Compliance

The Postal Service ensures compliance with information security policies through processes that include, but are not limited to, the following:

a. Regular testing of security systems and processes.

b. Vulnerability scans.

c. Inspections, reviews, and evaluations.

d. Monitoring.

e. Audits.

f. Confiscation and removal of information resources.

14-2.1 Regular Testing of Security Systems and Processes

Systems, processes, and custom software must be tested regularly because hackers and others continually discover vulnerabilities introduced in new software inadvertently by employees, contractors, and business partners. How testing is conducted is described in Exhibit 14-2.1.

Exhibit 14-2.1
Regular Testing of Security Systems and Processes

Frequency	Testing Activities
Continuously	Monitor all network traffic and alert personnel to suspected compromises using network intrusion-detection systems, host-based intrusion detection systems, and intrusion-prevention systems.
Weekly	Use file integrity monitoring software to alert personnel when files have been modified without authorization. Configure software so it can compare files.
Quarterly	Use a wireless analyzer to identify all wireless devices in use. Scan for vulnerabilities in internal and external networks (or when system components have been added, network topology has changed, firewall rules have been modified, or products have been updated).
Annually	Test security controls, limitations, network connections, and restrictions to identify unauthorized access attempts. Perform network-layer penetration testing (or when the infrastructure has been upgraded or modified (i.e., the operating system has been upgraded or a subnetwork or Web server has been added). Perform application-layer penetration testing (or when an application has been modified).

14-2.2 Vulnerability Scans

The Corporate Information Security Office Information Systems Security (CISO ISS) conducts vulnerability scans on applications, infrastructure components, and facilities.

14-2.3 Inspections, Reviews, and Evaluations

Inspections, reviews, and evaluations must be conducted for information resources and facilities to ensure compliance with Postal Service information security policies. A process is in place to monitor internal control compliance on an ongoing basis.

The CISO conducts inspections, reviews, and evaluations of information resources:

a. As part of the certification and accreditation (C&A) process.

b. When informally or formally requested by the supervisor or manager of an information resource.

c. At the discretion of the CISO or the VP IT Operations as necessary to evaluate the security of information resources.

The Inspection Service and/or CISO conducts inspections, reviews, and evaluations of Postal Service facilities.

14-3 Monitoring

Monitoring is used to improve security for Postal Service information resources to ensure appropriate use of those resources and to protect Postal Service resources from attack. Use of Postal Service information resources constitutes permission to monitor that use. Nonbusiness (i.e., personal) information may be viewed when monitoring Postal Service information resources.

All personnel are advised that the information on Postal Service nonpublicly available information resources may be monitored and viewed by appropriate, authorized personnel, regardless of privacy concerns. The Postal Service reserves the right to do the following:

a. Review the information contained in or traversing Postal Service information resources.

b. Review the activities on such information resources.

c. Act on information discovered as a result of monitoring and disclose this information to law enforcement and other organizations as deemed appropriate by Postal Service personnel.

14-3.1 What Is Monitored

Monitoring of Postal Service information resources may include, but is not limited to, the following:

a. Network traffic.

b. Application and data access.

c. Keystrokes and user commands.

d. E-mail and Internet usage.

e. Message and data content.

14-3.2 User Agreement to Monitoring

Any use of Postal Service information resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of Postal Service information resources:

a. Agree to comply with Postal Service policy concerning the use of information resources.

b. Acknowledge that their activities may be subject to monitoring.

c. Acknowledge that any detected misuse of Postal Service information resources may be subject to disciplinary action and prosecution pursuant to the United States Criminal Code (Title 18 U.S.C. § 1030).

14-3.3 User Monitoring Notification

Where possible, users are notified by the display of an authorized Postal Service warning banner (see Exhibit 14-3.3) that the information on Postal Service networks and workstations may be monitored and viewed by authorized personnel, regardless of privacy concerns.

The Postal Service-authorized warning banner must be displayed to users prior to granting session access to Postal Service information resources and be included in information security awareness training. The legal authority and obligations as indicated in the warning banner will apply throughout the entire session users have on the Postal Service information resources.

Applications that are single sign-on (SSO) or single log-on (SLO) compliant are not required to display an additional warning banner page as long as the executive sponsor can guarantee the user will see a warning banner at login for the session. Applications that are not SSO or SLO compliant must display a warning banner page.

Internal warning banners are not intended for display on Postal Service externally facing Internet Web sites where the Postal Service Internet privacy policy applies.

At a minimum, the warning banner must accomplish the following:

a. Identify the computer system as a Postal Service computer system protected by the United States Criminal Code.

b. Provide notification of monitoring.

c. Be followed by a pause requiring manual intervention to continue.

d. Identify the information resource as a Postal Service information resource and alert users that they have no expectation of privacy.

e. Warn users that activities may be monitored and that unauthorized access is prosecutable pursuant to the United States Criminal Code (Title 18 U.S.C. § 1030).

Note: Deviations from the authorized standard warning banner are not allowed unless approved in writing by the manager, CISO.

Exhibit 14-3.3
Authorized Standard Postal Service Warning Banner

WARNING! FOR OFFICIAL USE ONLY…

This is a U.S. Government computer system and is intended for official and other authorized use only. Unauthorized access or use of this system may subject violators to administrative action, civil, and/or criminal

prosecution under the United States Criminal Code (Title 18 U.S.C. § 1030).

All information on this computer system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy using this system. Any authorized or unauthorized use of this computer system signifies consent to and compliance with Postal Service policies and these terms.

I agree.

14-3.4 Requesting User Monitoring

Requests for monitoring network traffic, application and data access, keystrokes and user commands, and e-mail and Internet usage must be in writing and directed to the manager, CISO.

Requests for monitoring message and data content must be in writing and directed to the chief privacy officer (CPO).

14-3.5 Approving User Monitoring

The manager, CISO, has the responsibility to authorize in writing monitoring or scanning activities for network traffic, application and data access, keystrokes and user commands, and e-mail and Internet usage for Postal Service infrastructure or information resources. Personnel (except the Inspection Service and OIG) must receive authorization from the CISO prior to conducting monitoring and scanning activities.

The CPO has the responsibility to authorize, in writing, requests for message and data content monitoring.

In case of threats to the Postal Service infrastructure, network, or operations, the manager, CISO, is authorized to take appropriate action, which may include viewing and/or disclosing data to protect Postal Service resources or the nation's communications infrastructure.

14-3.6 Infrastructure Monitoring

The manager, CISO, is responsible for ensuring the security of the Postal Service infrastructure through the following:

a. Providing security incident detection through perimeter virus scanning, intrusion-detection services, and security event correlation tools.

b. Performing network vulnerability analyses.

c. Monitoring the Postal Service infrastructure, investigating incidents, and resolving and reassigning incidents to the appropriate group in a timely manner.

14-3.7 Intrusion Detection

Intrusion-detection devices are implemented to monitor the infrastructure. The use of all monitoring devices, except those used by the OIG, must be approved by the manager, CISO ISS. Unauthorized installation and use of monitoring devices are strictly prohibited.

14-4 Audits

14-4.1 Conducting Audits

The OIG has the authority to conduct audits, investigations, and evaluations of Postal Service programs and operations to ensure the efficiency and integrity of the Postal Service. The OIG coordinates investigative audits through the manager, CISO. Audits associated with financials [e.g., year-end

audits and Sarbanes-Oxley Act (SOX) audits] are coordinated through the SOX portfolio.

14-4.2 Responding to Audits

Corporate management responsible for the audited information resource must respond to internal and external audit findings and ensure that the information resources under their control comply with Postal Service information security policies and procedures.

14-5 Confiscation and Removal of Information Resources

The CISO, OIG, Inspection Service, or their designee may confiscate and remove any information resource suspected to be the object of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be used in forensic analysis of a security incident. The CISO, OIG, Inspection Service, or their designee, as appropriate, ensure that the chain of evidence (associated with the possession of the confiscated information resource) is preserved and documented.