Contents

1 Introduction. 1

2 Security Requirements 3

2-1 Data Security 3
2-2 Access Control 4
2-3 Security Awareness and Training 4
2-4 Audit and Accountability. 5
2-5 Configuration Management 5
2-6 Identification and Authentication 6
2-7 Incident Response 6
2-8 Maintenance 7
2-9 Media Protection 7
2-10 Personnel Security 8
2-11 Physical Protection 8
2-12 Risk Assessment 8
2-13 Security Assessment 9
2-14 System and Communications Protection 9
2-15 System and Information Integrity 10

3 Compliance 11

3-1 United States Postal Service Enforcement and Monitoring 11
3-2 Remediation 11
3-3 Audits and Certifications. 12

This page intentionally left blank

1 Introduction

The United States Postal Service® relies on the integrity, confidentiality, and availability of its information and information resources to conduct its business and fulfill its obligations to the public. Suppliers must create and maintain an environment that protects Postal Service™ information and information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. This document summarizes the security requirements necessary for protecting the confidentiality, integrity, and availability of Postal Service information and information systems that collect, process, store, or transmit Postal Service information. Further, this document supports practices set forth in the United States Postal Service security policies, as well as the Supplying Principles and Practices, available at *http://about.usps.com/manuals/pm/welcome.htm*.

The security requirements in this handbook apply to all suppliers and subcontractors whose business requires the accessing, processing, storage, or transmission of Postal Service information or interconnections to Postal Service networks and information systems.

This page intentionally left blank

2 Security Requirements

The Postal Service requires the security measures described in this handbook to ensure the confidentiality, integrity, and availability of Postal Service information and information resources.

2-1 Data Security

Postal Service policy provides specific guidelines for handling the various levels of sensitive and critical data. The following guidelines are not an exhaustive set of data security requirements and the Postal Service may require special or additional security measures:

a. Limit hard copy and electronic distribution to persons on a specific, job-related need-to-know basis.

b. Destroy data that is no longer needed or remains past its retention date.

c. Retain sensitive information in accordance with a retention schedule, where applicable.

d. Encrypt Postal Service information in storage (i.e., at rest), in transit, or stored off-site.

The Postal Service does not permit the following:

a. Storage of Postal Service information on devices not owned by the Postal Service.

b. Co-mingling of Postal Service information with information from sources other than the Postal Service.

c. Removal of Postal Service information from Postal Service premises without approval in writing from the functional vice president (data steward) and chief information officer or their designees.

d. Printing Postal Service information on printers where unauthorized people may see the output.

e. Using e-mail, IM, chat, etc. or other electronic means to send Postal Service information unless it is encrypted.

f. Discussing Postal Service information in an open area where others might overhear the conversation.

g. Transmitting Postal Service information by facsimile without appropriate approval.

2-2 Access Control

Access control guidelines are the following:

a. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

b. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

c. Control the flow of Postal Service information in accordance with approved authorizations.

d. Implement separation of duties of individuals to reduce the risk of malevolent activities without collusion.

e. Employ the principle of least privilege, including for specific security functions and privileged accounts.

f. Use non-privileged accounts or roles when accessing non-security functions.

g. Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

h. Limit the number of allowed unsuccessful logon attempts.

i. Provide privacy and security notices consistent with applicable Postal Service information rules.

j. Use session lock with pattern-hiding displays to prevent access and viewing of data after periods of inactivity.

k. Automatically terminate a user session after a defined condition (e.g., maximum period of inactivity, time-of-day restrictions).

l. Monitor and control remote access sessions.

m. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

n. Route remote access via managed access control points.

o. Authorize remote execution of privileged commands and remote access to security-relevant information.

p. Authorize wireless access prior to allowing such connections.

q. Protect wireless access using authentication and encryption.

r. Control connection of mobile devices.

s. Encrypt Postal Service information on mobile devices and mobile computing platforms.

t. Verify and control/limit connections to and use of external systems.

u. Limit use of organizational portable storage devices on external systems.

2-3 Security Awareness and Training

Security awareness and training guidelines are as follows:

a. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, guidelines, and procedures related to the security of those systems.
b. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
c. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

2-4 Audit and Accountability

Audit and accountability guidelines are as follows:

a. Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
b. Ensure that the actions of individual system users can be uniquely traced.
c. Review and update logged events.
d. Alert appropriate personnel in the event of an audit process failure.
e. Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
f. Provide audit reduction and report generation to support on-demand analysis and reporting.
g. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
h. Protect audit information and audit tools from unauthorized access, modification, and deletion.
i. Limit management of audit functionality to a subset of privileged users.

2-5 Configuration Management

Configuration management guidelines are as follows:

a. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the system development life cycle.
b. Establish and enforce security configuration settings for IT products employed in organizational systems.
c. Track, review, approve/disapprove, and audit changes to organizational systems.
d. Analyze the security impact of changes prior to implementation.

e. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

f. Employ the principle of least privilege by configuring organizational systems to provide only essential capabilities.

g. Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.

h. Apply deny-by-exception (block) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (allow) policy to allow the execution of authorized software.

i. Control and monitor user-installed software.

2-6 Identification and Authentication

Identification and authentication guidelines are as follows:

a. Identify system users, processes acting on behalf of users, and devices.

b. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.

c. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

d. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

e. Prevent reuse of identifiers for a defined period.

f. Disable identifiers after a defined period of inactivity.

g. Enforce a minimum password complexity and change of characters when passwords are created.

h. Prohibit password reuse for a specified number of generations.

i. Allow temporary password use for system logons with an immediate change to a permanent password.

j. Store and transmit only cryptographically protected passwords.

k. Obscure feedback of authentication information.

2-7 Incident Response

Incident response guidelines are as follows:

a. Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

b. Test the organizational incident response capability.

c. Track, document, and report incidents to appropriate Postal Service officials and/or authorities both internal and external to the organization.

d. Immediately report information security incidents and suspected security incidents, including privacy-related incidents, to the Postal Service Corporate Information Security Office (CISO) at 1-866-877-7247, in alignment with contractual obligations

2-8 Maintenance

Maintenance guidelines are as follows:

a. Perform maintenance on organizational systems.

b. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

c. Ensure equipment removed for off-site maintenance is sanitized of any Postal Service information.

d. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

e. Require multifactor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when non-local maintenance is complete.

f. Supervise the maintenance activities of maintenance personnel lacking access authorization.

2-9 Media Protection

Media protection guidelines are as follows:

a. Protect (i.e., physically control and securely store) system media containing Postal Service information, both paper and digital.

b. Limit access to Postal Service information on system media to authorized users.

c. Sanitize or destroy system media containing Postal Service information before disposal or release for reuse.

d. Mark media with prescribed Postal Service information markings and distribution limitations based on the classification level of the data contained thereon.

e. Control access to media containing Postal Service information and maintain accountability for media during transport outside of controlled areas.

f. Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.

g. Control the use of removable media on system components.

h. Prohibit the use of portable storage devices when such devices have no identifiable owner.

i. Protect the confidentiality of backup Postal Service information at storage locations.

2-10 Personnel Security

Personnel security guidelines are as follows:

a. Screen individuals prior to authorizing access to organizational systems containing Postal Service information.

b. Ensure that Postal Service information and organizational systems containing Postal Service information are protected during and after personnel actions such as terminations and transfers.

2-11 Physical Protection

Physical protection guidelines are as follows:

a. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

b. Protect and monitor the physical facility and support infrastructure for organizational systems.

c. Escort visitors and monitor visitor activity.

d. Maintain audit logs of physical access.

e. Control and manage physical access devices.

f. Enforce safeguarding measures for Postal Service information at alternate work sites.

2-12 Risk Assessment

Risk assessment guidelines are as follows:

a. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Postal Service information.

b. Scan for vulnerabilities in organizational systems and applications periodically or when new vulnerabilities affecting those systems and applications are identified.

c. Remediate vulnerabilities in accordance with risk assessments.

2-13 Security Assessment

Security assessment guidelines are as follows:

a. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

b. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

c. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

d. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

2-14 System and Communications Protection

System and communications protection guidelines are as follows:

a. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

b. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

c. Separate user functionality from system management functionality.

d. Prevent unauthorized and unintended information transfer via shared system resources.

e. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

f. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

g. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

h. Implement cryptographic mechanisms to prevent unauthorized disclosure of Postal Service information during transmission unless otherwise protected by alternative physical safeguards.

i. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

j. Establish and manage cryptographic keys for cryptography employed in organizational systems.

k. Employ FIPS-validated cryptography when used to protect the confidentiality of Postal Service information.

l. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

m. Control and monitor the use of mobile code.

n. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

o. Protect the authenticity of communications sessions.

p. Protect the confidentiality of Postal Service information at rest.

2-15 System and Information Integrity

System and information integrity guidelines are as follows:

a. Identify, report, and correct information and system flaws in a timely manner.

b. Implement a patch management program to ensure that security patches, hot fixes, and updated are implemented in a timely manner commensurate with the risk.

c. Provide protection from malicious code at appropriate locations within organizational systems.

d. Monitor system security alerts and advisories and take appropriate actions in response.

e. Update malicious code protection mechanisms when new releases are available.

f. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

g. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

h. Identify unauthorized use of organizational systems.

3 Compliance

3-1 United States Postal Service Enforcement and Monitoring

The Postal Service requires the contractual right to monitor and audit the performance of suppliers and subcontractors who collect, process, store, or transmit Postal Service information for compliance with Postal Service policies and requirements.

The Postal Service monitors supplier compliance with information security policies through processes that include, but are not limited to, the following:

a. **Supplier Security Assessments** - The Postal Service reserves the right to perform security assessments on suppliers. These assessments will occur no more than once annually unless a security incident has occurred, or the scope of the engagement between the Postal Service and the supplier has changed.

b. **Regular Testing of Security Systems and Processes** - Suppliers must test their systems, processes, and custom software regularly. Test results must be made available to Postal Service upon request.

c. **Vulnerability Scans** - Suppliers must conduct vulnerability scans on their applications, infrastructure components, and facilities at least monthly to ensure all system components meet security guidelines. Results must be made available to the Postal Service upon request.

d. **Inspections, Reviews, and Evaluations** - Suppliers must conduct inspections, reviews, and evaluations of information resources and facilities at least annually to ensure compliance with Postal Service information security policies. Results must be made available to the Postal Service upon request.

3-2 Remediation

During the aforementioned assessments and monitoring, should vulnerabilities be identified by the Supplier or Postal Service, the supplier is responsible for remediating the vulnerabilities, at their expense, in a timeframe commensurate with the criticality.

3-3 Audits and Certifications

To show compliance with Postal Service information security requirements, suppliers may submit reports generated by credible third-party auditing authorities. These reports may be used as evidence of compliance, but do not necessarily replace other Postal Service monitoring activities, listed above. Examples of acceptable evidence include the following:

a. Service Organization Control 2 Type II (SOC 2 Type II).

b. International Organization for Standardization (ISO 27001).

c. National Institute of Standards (NIST 800-53).

d. Federal Information Security Management Act (FISMA).

e. Payment Card Industry Data Security Standard (PCI/DSS) and/or Payment Application Data Security Standard (PA/DSS).