

Update Notice

Handbook AS-805, *Information Security* March 2002

This online version of Handbook AS-805, *Information Security*, published in March 2002, is updated through November 23, 2006, with the following *Postal Bulletin* articles:

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
Transmittal Letter				
C.	Distribution	insert correct URL.	22190	09-28-2006
D.	Comments and Questions	insert correct e-mail address. correct ordering information	22190	09-28-2006
Chapter 3, Information Designation and Control				
3-3.3.2	Business Impact Assessment Process	delete item g.	22190	09-28-2006
3-5.1.1	Sensitive Information	expand the number of hardcopy items to be labeled as restricted. add print screen to hardcopy labeled "restricted information."	22190	09-28-2006
3-5.1.2	Business-Controlled Sensitive Information	include a list of hardcopy items to be labeled as restricted.	22190	09-28-2006
3-5.1.1	Sensitive Information	update the requirements for labeling computer screen displays.	22160	08-04-2005
3-5.1.2	Business-Controlled Sensitivity Information	update the requirements for labeling computer screen displays.	22160	08-04-2005
3-5.1.1	Sensitive Information	remove screen display requirement.	22155	05-26-2005
3-5.1.2	Business-Controlled Sensitivity Information	remove screen display requirement.	22155	05-26-2005
3-5.2	Retention of Information	change reference from ASM 35 to Handbook AS-353.	22190	09-28-2006
3-5.3	Storage of Information	expand restrictions on prohibited actions.	22190	09-28-2006
3-5.3.1	Sensitive Information	explain how to store sensitive information.	22190	09-28-2006
3-5.3.2	Business-Controlled Sensitive, Critical, and Business-Controlled Critical Information	revise title by changing "sensitivity" to "sensitive" and "criticality" to "critical"; explain how to store sensitive information.	22190	09-28-2006

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
3-5.3.3	Isolation of Postal Service and Non-Postal Service Information	insert new section about keeping Postal Service information separate from non-Postal Service information.	22190	09-28-2006
3-5.4.1	Encryption of Information in Transit Across Networks	revise title from "Transmitted Across Untrusted Networks" to "Encryption of Information in Transit Across Networks"; change "sensitivity" to "sensitive."	22190	09-28-2006
3-5.4.2	Encryption of Information on Removable Devices or Media and in Offsite Storage	revise title from "Stored Onsite and Offsite" to "Encryption of Information on Removable Devices or Media and in Offsite Storage"; change "sensitivity" to "sensitive."	22190	09-28-2006
3-5.4.3	Encryption of Payment Card Industry Information	insert new section about PIC.	22190	09-28-2006
3-5.5	Removal of Postal Service Information from Postal Service Premises	add new section about removing Postal Service information from Postal Service premises.	22190	09-28-2006
3-5.6	Release of Information	change reference from ASM 35 to Handbook 353.	22190	09-28-2006
3-5.7	Disposal and Destruction of Information and Media	renumber from 3-5.6.	22190	09-28-2006
3-5.7.3	Disposal of Nonelectronic Information	change reference from ASM 35 to Handbook 353.	22190	09-28-2006
3-5.8.1	Sensitive and Business-Controlled Sensitive Information	revise title by changing "sensitivity" to "sensitive."	22190	09-28-2006
Chapter 5 Acceptable Use				
5-5.3	Using Approved Software	expand regulations for the safe use of software.	22190	09-28-2006
5-5.5	Protecting Postal Service Networks	delete the word "personal."	22190	09-28-2006
5-8	Generally Prohibited Uses of Postal Service Information Resources	insert "Postal Service" in title.	22190	09-28-2006
5-9	Prohibited Uses of Personal Information Resources	add new section on using personal devices.	22190	09-28-2006
5-10	Protection of Privacy	renumber from 5-9 to 5-10; add Handbook AS-353 as source of privacy guidelines.	22190	09-28-2006

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
5-10.3	Tracking Devices on Web Sites	revise title from "Privacy Policy Statements" to "Tracking Devices on Web Sites"; add www.usps.com as source for guidance on tracking devices.	22190	09-28-2006
5-10.5	Transfer to Another Site	delete reference to www.usps.com.	22190	09-28-2006
Chapter 6, Personnel Security				
6-2.4	All Managers	insert new items d and e, expanding manager responsibility; reletter items d through l as f through k.	22190	09-28-2006
6-2.4	All Managers	insert new items j and k, guidelines for handling departing personnel, and directing managers to MI AS-870-2005-2.	22190	09-28-2006
6-5.1	General Requirements	define the access permitted to information resources for personnel without security clearances.	22110	09-04-2003
6-5.2.1	Logon IDs	address the granting of logon IDs to personnel without security clearances.	22110	09-04-2003
6-7.3	Systems or Database Administrator Departure	insert new part with guidelines on procedures when administrators leave.	22190	09-28-2006
Chapter 7, Physical and Environmental Security				
7-2.6	All Personnel	update gaining access to controlled areas. Relettered current items b through e as new items d through g. Added new items b and c.	22164	09-29-2005
7-3.1.3	Access to Controlled Areas	update gaining access to controlled areas.	22164	09-29-2005
7-3.2	Physical Protection of Information Resources	expand the Note with guidance on encrypting information.	22190	09-28-2006
7-3.2.2	Postal Service Workstations and Portable Devices	add "Postal Service" to title; delete language about portable devices.	22190	09-28-2006
7-3.2.3	Non-Postal Service Portable Devices	revise title from "Non-Postal Service Personal Digital Assistants and Handheld Devices" to "Non-Postal Service Portable Devices"; expand guidelines on dealing with PDAs.	22190	09-28-2006
7-3.4	Facility Business Continuance Management Planning	update gaining access to controlled areas.	22164	09-29-2005
Chapter 8, System, Applications, and Product Development				

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
Exhibit 8-2	System, Application, and Product Development Responsibilities	change exhibit table.	22153	04-28-2005
Exhibit 8-2	System, Application, and Product Development Responsibilities	update the facility business continuance management planning section.	22164	09-29-2005
Chapter 8, System, Applications, and Product Development				
Exhibit 8-6	Overview of ISA Phases for Applications	change exhibit table.	22153	04-28-2005
8-2.2	Vice President, Chief Technology Officer	update title and VP/CTO duties.	22153	04-28-2005
8-2.3	Vice President, Functional Business Areas	update VP/CTO duties.	22153	04-28-2005
8-2.4	Manager, Corporate Information Security Office	add new item d.	22153	04-28-2005
8-2.5	Executive Sponsors	add new item g.	22153	04-28-2005
8-2.6	Portfolio Managers	add item i; expanding portfolio manager's responsibility.	22190	09-28-2006
8-2.6	Portfolio Managers	add the responsibility for registering the information resource in eAccess.	22110	09-04-2003
8-2.6	Portfolio Managers	change title from "Portfolio/Business Managers" to "Portfolio Managers" and duties.	22153	04-28-2005
8-2.6	Portfolio Managers	address implementing an acceptance of responsibility letter for documented vulnerabilities that will not be mitigated. Relettered current items e through g as new items f through h. Added new item e.	22164	09-29-2005
8-2.7	Managers/Computing Operations Infrastructures	delete this section and renumber remaining sections.	22153	04-28-2005
8-2.8	Accreditor	update title and duties.	22153	04-28-2005
8-2.9	Certifier	update title and duties.	22153	04-28-2005
8-2.10	Information Systems Security Officers	change ISA documentation receipt to certifier.	22153	04-28-2005
8-2.11	Information Systems Security Representatives	change management duties.	22153	04-28-2005
8-3.6.2	Testing with Nonsensitive Production Data	change management duties.	22153	04-28-2005
8-3.6.3	Testing with Sensitive and Business-Controlled Sensitivity Production Data	change management duties.	22153	04-28-2005

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
8-5	Information Security Assurance Process	add application or infrastructure component.	22153	04-28-2005
8-5.1	What the ISA Process Covers	add sentence about need for wireless products to be part of ISA process.	22190	09-28-2006
8-5.1	What the ISA Process Covers	change the frequency from every 3 years to 5 years.	22153-	04-28-2005
8-6	Application Information Security Assurance Phases	update title.	22153	04-28-2005
8-6.1.1	Initiate Application Information Security Assurance Process	update title and text to include applications.	22153	04-28-2005
8-6.1.2	Assign Information Systems Security Representative	include Portfolio Manager.	22153	04-28-2005
Chapter 8, System, Applications, and Product Development				
8-6.1.3	Conduct Business Impact Statement	remove RTO.	22153	04-28-2005
8-6.1.4	Define Security Requirements	include applications and remove information resources.	22153	04-28-2005
8-6.1.5	Document High-Level Architecture	update the facility business continuance management planning section.	22164	09-29-2005
8-6.1.6	Document Information Resources in the Enterprise Information Repository	update the facility business continuance management planning section.	22164	09-29-2005
8-6.2	Phase 2 - Design and Integration	include applications and remove information resources.	22153	04-28-2005
8-6.2.1	Document High-Level Architecture	include applications and remove information resources.	22153	04-28-2005
8-6.2.1	Document High-Level Architecture	update the facility business continuance management planning section. Deleted 8-6.2.1, Document High-Level Architecture.	22164	09-29-2005
8-6.2.2	Document Information Resources in the Enterprise Information Repository	include applications and remove information resources.	22153	04-28-2005
8-6.2.2	Document Information Resources in the Enterprise Information Repository	update the facility business continuance management planning section. Deleted 8-6.2.2, Document Information Resources in the Enterprise Information Repository.	22164	09-29-2005
8-6.2.3	Conduct Risk Assessment	include applications and remove information resources.	22153	04-28-2005
8-6.2.4	Identify Security Controls	include applications and remove information resources.	22153	04-28-2005

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
8-6.2.5	Perform Controls Analysis	include applications and remove information resources.	22153	04-28-2005
8-6.2.6	Perform Cost Benefit Analysis	include applications and remove information resources.	22153	04-28-2005
8-6.2.8	Develop Security Plan	include applications and remove information resources.	22153	04-28-2005
8-6.2.10	Harden Information Resources	include applications and remove information resources.	22153	04-28-2005
8-6.2.11	Conduct Vulnerability Scan	add new section regarding application vulnerability.	22153	04-28-2005
8-6.2.11	Conduct Vulnerability Scan	update the facility business continuance management planning section. Deleted 8-6.2.11, Conduct Vulnerability Scan.	22164	09-29-2005
Chapter 8, System, Applications, and Product Development				
8-6.2.12	Develop Application Disaster Recovery Plan	update title and include an application recovery plan.	22153	04-28-2005
8-6.2.13	Develop Facility Recovery Plan	change management duties.	22153	04-28-2005
8-6.2.14	Develop Standard Operating Procedures	include applications and remove information resources.	22153	04-28-2005
8-6.2.14	Register Application in eAccess	address registering applications in eAccess. Renumbered current 8-6.2.3 through 8-6.2.16 as new 8-6.2.1 through 8-6.2.13. Added new 8-6.2.14.	22164	09-29-2005
8-6.2.15	Incorporate Security Requirements in SLAs and Trading Partner Agreements	include applications and remove information resources.	22153	04-28-2005
8-6.2.16	Develop Operational Security Training	include applications and remove information resources.	22153	04-28-2005
8-6.3.1	Develop Security Test Plan	include applications and remove information resources.	22153	04-28-2005
8-6.3.2	Conduct Operational Security Training	update title and include applications and remove information resources.	22153	04-28-2005
8-6.3.3	Conduct Security Code Review	include applications and remove information resources.	22153	04-28-2005
8-6.3.4	Conduct Vulnerability Scan	address implementing an acceptance of responsibility letter for documented vulnerabilities that will not be mitigated. Renumbered current 8-6.3.4 through 8-6.3.9 as new 8-6.3.5 through 8-6.3.10. Added new 8-6.3.4.	22164	09-29-2005

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
8-6.3.5.2	Criteria for Conducting an Independent Security Code Review	include applications and remove information resources and update management duty.	22153	04-28-2005
8-6.3.6	Conduct Security Testing and Document Results	include applications and remove information resources.	22153	04-28-2005
8-6.3.6.2	Criteria for Conducting an Independent Security Code Review	revise item c to delete words "trusted" and replace word "untrusted" with "external" network.	22190	09-28-2006
8-6.3.7.2	Criteria for Conducting Independent Penetration Testing and Vulnerability Scans	include applications and remove information resources and update management duty.	22153	04-28-2005
8-6.3.8.1	Independent Validation of Security Testing Description	include applications and remove information resources.	22153	04-28-2005
8-6.3.8.2	Criteria for Conducting Independent Validation of Security Testing	include applications and remove information resources and update management duty.	22153	04-28-2005
8-6.3.9	Address Outstanding Issues	include applications and remove information resources.	22153	04-28-2005
8-6.4	Phase 4 - Evaluation	include applications and remove information resources.	22153	04-28-2005
Chapter 8, System, Applications, and Product Development				
8-6.4.1	Develop ISA Documentation Package	include applications and remove information resources.	22153	04-28-2005
8-6.4.2	Review ISA Documentation Package and Write Evaluation Report	update section with ISSO duties.	22153	04-28-2005
8-6.4.3	Escalate Security Concerns or Certify Application	add new section to include certifier duties.	22153	04-28-2005
8-6.4.4	Escalate Security Concerns or Prepare Risk Mitigation Plan	add new section to portfolio manager duties.	22153	04-28-2005
8-6.4.5	Escalate Security Concerns or Accredited Application	update title and accreditor duties.	22153	04-28-2005
8-6.4.6	Make Decision to Deploy (or Continue to Deploy) or Return for Rework	update title and manager duties.	22153	04-28-2005
8-6.4.7	Deploy Application	include applications and remove information resources.	22153	04-28-2005
8-6.5	Phase 5 - Production	include applications and remove information resources.	22153	04-28-2005
8-6.5.1	Follow Security-Related Plans and Continually Monitor Operations	include applications and remove information resources.	22153	04-28-2005
8-6.5.2	Periodically Review, Test, and Audit	include applications and remove information resources.	22153	04-28-2005

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
8-6.5.3	Re-assess Risks and Upgrade Security Controls	change the frequency from every 3 years to 5 years.	22153	04-28-2005
8-6.5.5	Re-initiate ISA	delete word "primary" in item a (1); item c, add word "A" to beginning of sentence.	22190	09-28-2006
8-6.5.5	Re-initiate ISA	change the frequency from every 3 years to 5 years, include applications, and remove information resources.	22153	04-28-2005
8-6.5.7.1	Disposal of Data	revise title from "Shutdown and Disposal of Data" to "Disposal of Data"; change reference from ASM 35 to Handbook-353.	22190	09-28-2006
Chapter 9, Information Security Services				
9-4.1.1	Clearances	define the access permitted to information resources for personnel without security clearances.	22110	09-04-2003
9-4.2	Authorization Process	add sentence about eAccess.	22190	09-28-2006
9-4.2.1	Baseline Information Services	show what information services may be authorized for individuals without an appropriate personnel clearance, what services are not available, and that baseline access must be set to expire every 3 months.	22110	09-04-2003
9-4.2.2	Requesting Authorization	identify the eAccess process.	22110	09-04-2003
9-4.2.3	Approving Requests	define the need to register applications in eAccess.	22110	09-04-2003
9-5.2.3	Individual Accountability	change word "authenticate" to "verify" in item b.	22190	09-28-2006
9-5.3	Types of Accounts	add items e and f.	22190	09-28-2006
9-5.3	Types of Accounts	group the types of accounts and to add a section to address generic accounts.	22105	06-26-2003
9-5.4.3	Configuring Account Time-outs	change time-outs from 15 minutes to every 30 minutes.	22149	03-03-2005
9-5.4.4	Departing Personnel	address the issue of departing personnel.	22105	06-26-2003
9-7.1.1	Password Selection Requirements	revise items a and b to expand guidelines for selecting passwords.	22190	09-28-2006
9-7.1.1	Password Selection Requirements	bring password requirements into alignment with current Postal Service needs.	22099	04-03-2003

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
9-7.1.4	Password Suspension	add language about unsuccessful password attempts.	22190	09-28-2006
9-7.1.5	Re-set Passwords	expand guidelines for re-setting passwords.	22190	09-28-2006
9-7.1.5	Password Expiration	bring password requirements into alignment with current Postal Service needs.	22099	04-03-2003
9-7.1.7	Requests for Use of Non-Expiring Password Accounts	add new section about requesting non-expiring passwords.	22190	09-28-2006
9-7.1.11	Password Requirements	add new item b about suspending or disabling account; reletter items b through d as new items c through e.	22190	09-28-2006
9-7.4.1	Digital Certificates	revise 2nd sentence, adding word "decryption."	22190	09-28-2006
9-7.9.3	Time-out Requirements (Reauthentication)	change time-outs from 15 minutes to every 30 minutes.	22149	03-03-2005
9-7.9.3.1	Workstations	address inactivity time-out standards for workstations.	22114	10-30-2003
		change time-outs from 15 minutes to every 30 minutes.	22149	03-03-2005
9-7.9.3.2	Applications	address inactivity time-out standards for applications.	22114	10-30-2003
9-7.9.3.3	Remote Access	address inactivity time-out standards for remote access.	22114	10-30-2003
9-8.2	Encryption	revise last sentence to include AES.	22190	09-28-2006
9-8.2.1	Required for Transmission and Storage on Removable Devices and Media	revise title from "Required for Nonsecure Storage and Transmission over Untrusted Networks" to "Required for Transmission and Storage on Removable Devices and Media"; revise last sentence; add language about encryption requirements.	22190	09-28-2006
9-8.2.2	Recommended for Storage on Non-Removable Devices	revise title from "Recommended for Secure Storage" to "Recommended for Storage on Non-Removable Devices"; replace "sensitivity" with "sensitive; add encryption reference.	22190	09-28-2006
9-10.4	High Availability	reletter items d through g as f through i; add new items d and e.	22190	09-28-2006

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
9-12	Audit Logging	revise introductory text to clarify meaning of audit logs.	22190	09-28-2006
9-12.5	Audit Log Retention	change reference from ASM 35 to Handbook AS-353.	22190	09-28-2006
Chapter 10, Hardware and Software Security				
10-2.8	Database Administrators	address implementing patch management of information resources. Revised item d.	22164	09-29-2005
10-4.5	Patch Management	address implementing patch management of information resources. Renumbered current 10-4.5 through 10-4.6 as new 10-4.6 through 10-4.7. Added new 10-4.5.	22164	09-29-2005
10-5.3.3	Using Database Servers	address hosting Web and database servers on the same information resource.	22109	08-21-2003
10-5.3.4	Combined Web and Database Servers	present the requirements for hosting Web and database servers on the same information resource.	22109	08-21-2003
10-5.4	Workstations	address mandatory workstation connectivity.	22149	03-03-2005
10-5.4.2	Password- or Token-Protected Screen Saver	revise title from "Screen Savers and Screen Locking" to "Password- or Token-Protected Screen Savers."	22190	09-28-2006
10-5.4.2	Screen Savers and Screen Locking	change time-outs from 15 minutes to every 30 minutes.	22149	03-03-2005
10-5.5	Portable Devices	address mandatory workstation connectivity.	22149	03-03-2005
10-6.3.4	Unapproved Software	add section on unapproved software.	22190	09-28-2006
10-6.6.1	DBMS Activity Logs	replace phrase "continuity and contingency planning" with "continuance management."	22190	09-28-2006
10-7.1.1	Installation	delete words "after installation."	22190	09-28-2006
10-7.2.6	Spyware Protection Measures	add new section about spyware.	22190	09-28-2006
Chapter 11 Networks and Communications				
11-3.1	Purpose	add word "confidentiality" to introductory text.	22190	09-28-2006
11-5.10	Isolation of Postal Service and Non-Postal Service Networks	add language about isolating networks.	22190	09-28-2006

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
11-12.1	Authentication	revise last sentence, remove word "sensitivity," and delete language about untrusted network.	22190	09-28-2006
Chapter 12, Business Continuance Management				
		establish Postal Service BCM requirements.	22138	09-30-2004
Exhibit 12.2.	Business Continuance Management Responsibilities	change entry in one cell.	22190	09-28-2006
12-2.11	Executive Sponsors	add new item c (old c becomes d).	22190	09-28-2006
12-6	Relationship of Criticality, Recovery Time Objective, and Recovery Point Objective	expand instructions on RTO.	22190	09-28-2006
Chapter 13, Incident Management				
		provide requirements related to information security incidents that threaten the integrity, availability, or confidentiality of Postal Service information resources.	22138	09-30-2004
13-3.2	Reportable Incidents	reletter items m through w as n through x; add new item m about display of strange messages.	22190	09-28-2006
13-4	Incident Prevention	in item d, replace "install and maintain" with "use." Revise and reletter old items f through l.	22190	09-28-2006S
Chapter 14, Compliance and Monitoring				
Exhibit 14-5.4	Authorized Standard Postal Service Warning Banner	remove boldface from last sentence of second paragraph.	22190	09-28-2006S
14-5.5	Warning Banner	update warning banner information.	22155	05-26-2005
14-5.6.1	Requesting User Monitoring	revise title from "Requesting Monitoring" to "Requesting User Monitoring."	22190	09-28-2006S
14-5.6.2	Approving User Monitoring	revise title from "Authorizing Monitoring" to "Approving User Monitoring."	22190	09-28-2006S
14-5.7	Infrastructure Monitoring	replace "SIS" with "CISO."	22190	09-28-2006S
14-7	Confiscation and Removal of Information Resources	expand number of parties permitted to confiscate information resources.	22190	09-28-2006S
Chapter 15, Wireless Networking				

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
		add new Chapter 15 that establishes the roles, responsibilities, and requirements to appropriately protect wireless solutions implemented for the Postal Service.	22147	02-03-2005
15-1	Policy	add third paragraph about wireless technology.	22190	09-28-2006
15-6.1	General	replace 2nd abbreviation "WLANs" with "wired networks."	22190	09-28-2006
15-9.3	Technical Security Requirements	revise and expand list of requirements.	22190	09-28-2006
Appendix A, Consolidated Roles and Responsibilities				
		reflect responsibilities related to the revisions of chapters 13 and 14.	22138	09-30-2004
2	Vice President, Chief Technology Officer	update manager duties.	22153	04-28-2005
3	Manager, Corporate Information Security Office	include ISA information.	22153	04-28-2005
5	Vice Presidents, Functional Business Areas	update manager duties.	22153	04-28-2005
10	Executive Sponsors	include ISA information.	22153	04-28-2005
11	Portfolio Managers	add item k, about additional responsibility.	22190	09-28-2006
11	Portfolio Managers	update manager duties.	22153	04-28-2005
11	Portfolio Managers	update manager duties. Relettered current items e through i as new items f through j. Added new item e.	22164	09-29-2005
29	Accreditor	update title and manager duties.	22153	04-28-2005
30	Certifier	add new section to include certifier duties.	22153	04-28-2005
33	Information Systems Security Representatives	include portfolio manager duties.	22153	04-28-2005
35	Database Administrators	address implementing patch management of information resources. Updated item l.	22164	09-29-2005
Appendix A, Consolidated Roles and Responsibilities				
36	All Personnel	address implementing patch management of information resources. Relettered current items e through s as new items g through u. Added new items e and f.	22164	09-29-2005

This chapter, subchapter, part, or section...	titled...	was revised to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
Appendix B, Information Security and Related Documents				
Appendix B	Information Security and Related Documents	correct title of Pub 805-A	22190	09-28-2006
Appendix B	Information Security and Related Documents	update Appendix B.	22164	09-29-2005
Glossary				
		delete this section. It will be published on the IT Web site only, under Corporate Information Security.	22138	09-30-2004
Acronyms				
		delete this section. It will be published on the IT Web site only, under Corporate Information Security.	22138	09-30-2004



Information Security

Handbook AS-805

March 2002
Transmittal Letter

A. Purpose

Trust has always been a cornerstone of the Postal Service brand. As we increase our reliance on information systems to help us manage information, improve service, manage costs, and carry out our mission more efficiently, we have a greater responsibility than ever to preserve the trust of our customers, our employees, and those we do business with. Handbook AS-805, *Information Security*, provides the tools to help each of us do that.

B. Organization

Protecting information resources covers a broad spectrum of topics and responsibilities for our employees, vendors, and business partners. In this handbook, the topics have been associated with the responsibilities as follows:

- Chapter 2 presents high level roles and responsibilities for implementing the information security program and a table listing positions and the chapters where those positions have specific roles and responsibilities.
- Chapters 3 through 14 present specific roles and responsibilities associated with the chapter topic and an at-a-glance table of related information security activities.
- Appendix A presents a consolidation of all roles and responsibilities.

C. Distribution

This handbook is being distributed via paper to Headquarters officers and managers, area and district managers, the Postal Inspection Service, and the Office of the Inspector General and is available through the Postal Service PolicyNet page at <http://blue.usps.gov/cpim/hbkid.htm>. Additional copies may be ordered from the material distribution center (MDC) using Form 7380, *MDC Supply Requisition*.

D. Comments and Questions

Submit comments and questions to:

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

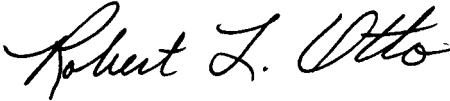
Comments may also be sent by e-mail to information_security@usps.gov.

Additional copies may be ordered from the Material Distribution Center (MDC) using touch tone order entry (TTOE). Call 800-273-1509.

Note: You must be registered to use TTOE. To register, call 800-332-0317; select option 8, extension 2925, and follow the prompts to leave a message. (Wait 48 hours after registering before placing your first order.)

E. Rescission

This handbook is a revision of Hbk. AS-805, *Information Systems Security*, April 1994. It obsoletes Hbk. AS-818, *Local Area Network and Personal Computer Security*, April 1994; MI AS-830-92-11, *Electronic Messaging System Policy*; MI AS-840-95-12, *Employee Access to the Internet*; MI AS-850-97-3, *Security Certification and Accreditation of Sensitive Applications and Systems*; and MI AS-870-90-7, *Computer Virus Guidelines*. Please recycle all copies of these documents.

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

Robert L. Otto
Vice President
Information Technology

Contents

1	Introduction	1
1-1	Policy	1
1-2	Purpose	1
1-3	Scope of Information Security Policies	2
1-3.1	Information Resources	2
1-3.2	Organizations and Personnel	2
1-4	Guiding Principles	4
1-5	Importance of Compliance	4
1-5.1	Maintaining Public Trust	4
1-5.2	Continuing Business Operations	4
1-5.3	Protecting Postal Service Investment	4
1-5.4	Abiding by Federal Regulations	5
1-6	Information Security and the Privacy Act	5
1-7	Information Security Program	5
2	Roles and Responsibilities	7
2-1	Policy	7
2-2	How Roles and Responsibilities Are Presented	7
2-3	Roles and Responsibilities Summary	9
2-3.1	Chief Inspector	9
2-3.2	Chief Information Officer/Vice President, Information Technology	9
2-3.3	Manager, Corporate Information Security Office	9
2-3.4	Chief Privacy Officer	9
2-3.5	Inspector General	9
2-3.6	Technology Managers	10
2-3.7	All Officers and Managers	10
2-3.8	All Personnel	10
3	Information Designation and Control	11
3-1	Policy	11
3-2	Roles and Responsibilities	11
3-2.1	Executive Sponsors	11
3-2.2	Manager, Corporate Information Security Office	12
3-2.3	Chief Privacy Officer	12
3-2.4	Portfolio/Business Managers	12
3-2.5	Information Systems Security Officers	12
3-2.6	Information Systems Security Representatives	13

3-2.7	Project Managers	13
3-2.8	All Personnel	13
3-2.9	Inspector General	13
3-3	Information Designation	14
3-3.1	Information Designation Categories and Levels	14
3-3.2	Sensitivity and Criticality Category Independence	14
3-3.3	Determination of Sensitivity and Criticality	15
3-3.3.1	Business Impact Assessment	15
3-3.3.2	Business Impact Assessment Process	15
3-3.3.3	Recording Information Resource Designation	15
3-4	Security Requirements	15
3-4.1	Security Requirements and Controls	15
3-4.2	Security Requirement Categories	16
3-4.3	Baseline Security Requirements	16
3-4.4	Mandatory Security Requirements	17
3-4.5	Discretionary Security Requirements	17
3-5	Handling Information and Media	17
3-5.1	Labeling of Information and Media	17
3-5.1.1	Sensitive Information	17
3-5.1.2	Business-Controlled Sensitive Information	18
3-5.2	Controlling Access to Information	18
3-5.3	Retention of Information	18
3-5.4	Storage of Information	18
3-5.4.1	Sensitive Information	18
3-5.4.2	Business-Controlled Sensitive, Critical, and Business-Controlled Critical Information	19
3-5.4.3	Isolation of Postal Service and Non-Postal Service Information	19
3-5.5	Encryption of Information	19
3-5.5.1	Encryption of Information in Transit Across Networks	19
3-5.5.2	Encryption of Information on Removable Devices or Media and in Offsite Storage	19
3-5.5.3	Encryption of Payment Card Industry Information	19
3-5.6	Removal of Postal Service Information from Postal Service Premises	19
3-5.7	Release of Information	20
3-5.7.1	Sensitive Information	20
3-5.7.2	Business-Controlled Sensitivity Information	20
3-5.7.3	Releasing Information on Factory-Fresh or Degaussed Media	21
3-5.7.4	Precautions Prior to Maintenance	21
3-6	Disposal and Destruction of Information and Media	21
3-6.1	Disposal of Electronic Hardware and Media	21
3-6.2	Removal of Data Residue	21

Contents

- 3-6.3 Disposal of Nonelectronic Information 22
- 3-7 Handling Contaminated Information Resources 22
 - 3-7.1 Sensitive and Business-Controlled Sensitive Information 22
 - 3-7.2 Data Eradication on Contaminated Information Resources 22
 - 3-7.3 Reporting of Contaminated Information Resources 22
- 3-8 Handling Non-Postal Service Information 23
 - 3-8.1 Third-Party Information 23
 - 3-8.2 National Security Classified Information 23
- 4 Risk Management 25**
 - 4-1 Policy 25
 - 4-2 Roles and Responsibilities 25
 - 4-2.1 Vice Presidents, Functional Business Areas 25
 - 4-2.2 Chief Information Officer/Vice President, Information Technology 25
 - 4-2.3 Executive Sponsors 26
 - 4-2.4 Portfolio/Business Managers 26
 - 4-2.5 Information Systems Security Representatives 26
 - 4-2.6 Manager, Corporate Information Security Office 26
 - 4-2.7 Information Systems Security Officers 26
 - 4-2.8 Installation Heads 27
 - 4-2.9 Chief Inspector 27
 - 4-2.10 Inspector General 27
 - 4-3 Types of Risk Management 28
 - 4-4 Information Resource Risk Management 28
 - 4-4.1 Information Resource Risk Assessment 28
 - 4-4.1.1 Purpose 28
 - 4-4.1.2 Frequency of Risk Assessment 28
 - 4-4.1.3 Re-assessments 28
 - 4-4.2 Information Resource Risk Mitigation 29
 - 4-4.3 Information Resource Risk Acceptance 29
 - 4-4.4 Information Resource Risk Management Documentation 29
 - 4-5 Independent Risk Management 30
 - 4-5.1 Independent Risk Assessment 30
 - 4-5.2 Criteria for Conducting Independent Risk Assessments 30
 - 4-6 Site Risk Management 30
 - 4-6.1 Site Security Review 30
 - 4-6.2 Frequency of Site Security Review 31
 - 4-6.3 Site Risk Mitigation 31
 - 4-6.4 Site Risk Acceptance 31
 - 4-6.5 Site Risk Management Documentation 31

5	Acceptable Use	33
5-1	Policy	33
5-2	Roles and Responsibilities	33
5-2.1	Chief Privacy Officer	33
5-2.2	Executive Sponsors	33
5-2.3	All Managers	34
5-2.4	Manager, Corporate Information Security Office	34
5-2.5	All Personnel	34
5-2.6	Inspector General	35
5-3	Monitoring	35
5-3.1	Right to Monitor	35
5-3.1.1	Use Constitutes Permission	35
5-3.1.2	Public Web Site Monitoring	36
5-3.2	Notification of Monitoring	36
5-4	Ensuring Compliance	36
5-5	Hardware and Software	36
5-5.1	Acquiring Hardware and Software	36
5-5.2	Complying with Copyright and Licensing	36
5-5.3	Using Approved Software	37
5-5.4	Protecting Intellectual Property	37
5-5.5	Protecting Postal Service Networks	37
5-6	Electronic Mail and Messaging	37
5-6.1	Acceptable Use	38
5-6.2	Prohibited Use	38
5-6.3	Encryption	38
5-6.4	Authorized Monitoring	39
5-7	Internet	39
5-7.1	Acceptable Use	39
5-7.2	Prohibited Use	39
5-8	Generally Prohibited Uses of Postal Service Information Resources	40
5-9	Prohibited Uses of Personal Information Resources	41
5-10	Protection of Privacy	41
5-10.1	Nonpublic Information Resources	41
5-10.2	Publicly Available Information Resources	41
5-10.3	Tracking Devices on Web Sites	41
5-10.4	Customer Data Collection	42
5-10.5	Transfer to Another Site	42
6	Personnel Security	43
6-1	Policy	43
6-2	Roles and Responsibilities	43

Contents

6-2.1	Chief Inspector	43
6-2.2	Manager, Corporate Information Security Office	43
6-2.3	Contracting Officers	44
6-2.4	All Managers	44
6-2.5	All Personnel	45
6-2.6	Inspector General	45
6-3	Employee Accountability	45
6-3.1	Separation of Duties and Responsibilities	45
6-3.1.1	Required for Sensitive or Critical Information Resources	45
6-3.1.2	Recommended for Business-Controlled Information Resources	46
6-3.2	Job Descriptions	46
6-3.3	Performance Appraisals	46
6-3.4	Condition of Continued Employment	46
6-3.5	Sanctions	46
6-4	Sensitive Positions	46
6-4.1	Definition of Sensitive Positions	46
6-4.2	Identification of Sensitive Positions	47
6-5	Background Investigations and Clearances	47
6-5.1	General Requirements	47
6-5.2	Access Privileges	47
6-5.2.1	Logon IDs	47
6-5.2.2	Sensitive Resources	47
6-5.2.3	Controlled Areas	47
6-5.3	Foreign Nationals	48
6-6	Information Security Awareness and Training	48
6-6.1	General Security Awareness	48
6-6.2	Annual Training	48
6-6.3	Information Resource Operational Security Training	48
6-6.4	New Personnel Training	48
6-7	Departing Personnel	48
6-7.1	Routine Separation	48
6-7.2	Adverse Termination	49
6-7.3	Systems or Database Administrator Departure	49
7	Physical and Environmental Security	51
7-1	Policy	51
7-2	Roles and Responsibilities	51
7-2.1	Chief Inspector	51
7-2.2	Manager, Corporate Information Security Office	52
7-2.3	Installation Heads	52
7-2.4	Security Control Officers	53

7-2.5	Contracting Officers	53
7-2.6	All Personnel	53
7-2.7	Inspector General	54
7-3	Facility Security	54
7-3.1	Physical Access Controls	54
7-3.1.1	Establishment of Controlled Areas	54
7-3.1.2	Types of Information Resources Stored in Controlled Areas	55
7-3.1.3	Access to Controlled Areas	55
7-3.1.4	Establishment of Access Control Lists	55
7-3.1.5	Training for Controlled Areas	55
7-3.1.6	Installation of Physical Access Control Devices	56
7-3.1.7	Implementation of Additional Physical Access Security	56
7-3.1.7.1	Required for Sensitive or Critical Information Resources	56
7-3.1.7.2	Recommended for Business-Controlled Information Resources	56
7-3.1.8	Implementation of Identification Badges	56
7-3.2	Physical Protection of Information Resources	56
7-3.2.1	Network Equipment, Network Servers, and Mainframes	57
7-3.2.2	Postal Service Workstations and Portable Devices	57
7-3.2.3	Non-Postal Service Portable Devices	57
7-3.2.4	Sensitive, Critical, and Business-Controlled Media	57
7-3.3	Environmental Security	57
7-3.4	Facility Business Continuance Management Planning	58
7-3.5	Facility Contracts	58
8	System, Applications, and Product Development	59
8-1	Policy	59
8-2	Roles and Responsibilities	59
8-2.1	Chief Inspector	59
8-2.2	Vice President, Chief Technology Officer	59
8-2.3	Vice Presidents, Functional Business Areas	60
8-2.4	Manager, Corporate Information Security Office	60
8-2.5	Executive Sponsors	60
8-2.6	Portfolio Managers	61
8-2.7	Project Managers	62
8-2.8	Accreditor	62
8-2.9	Certifier	62
8-2.10	Information Systems Security Officers	62
8-2.11	Information Systems Security Representatives	63
8-2.12	Contracting Officers and Contracting Officer Representatives	63
8-2.13	General Counsel	63
8-2.14	Business Partners	64

Contents

8-2.15	Chief Privacy Officer	64
8-2.16	Inspector General	64
8-3	General Development Concepts	65
8-3.1	Life Cycle Approach	66
8-3.2	Risk Management	66
8-3.3	Quality Assurance	66
8-3.4	Change Control, Version Control, and Configuration Management	66
8-3.5	Separation of Duties	67
8-3.6	Development and Test Environment Restrictions	67
8-3.6.1	Separation of Development/Test and Production Environments	67
8-3.6.2	Testing with Nonsensitive Production Data	67
8-3.6.3	Testing with Sensitive and Business-Controlled Sensitivity Production Data	67
8-3.6.4	Testing at Non-Postal Service Facilities with Production Data	67
8-4	Security Activities and the Development Life Cycle	68
8-5	Information Security Assurance Process	68
8-5.1	What the ISA Process Covers	68
8-5.2	When ISA Is Required	68
8-5.3	Value of the ISA Process to the Postal Service	68
8-5.4	Access to Information Resources and Related Documentation	69
8-5.5	Independent Processes	69
8-6	Application Information Security Assurance Phases	69
8-6.1	Phase 1 — Definition	69
8-6.1.1	Initiate Application Information Security Assurance Process	69
8-6.1.2	Assign Information Systems Security Representative	69
8-6.1.3	Conduct Business Impact Assessment	71
8-6.1.4	Define Security Requirements	71
8-6.1.5	Document High-Level Architecture	71
8-6.1.6	Document Information Resources in the Enterprise Information Repository	71
8-6.2	Phase 2 — Design and Integration	71
8-6.2.1	Conduct Risk Assessment	71
8-6.2.2	Identify Security Controls	72
8-6.2.3	Perform Controls Analysis	72
8-6.2.4	Perform Cost Benefit Analysis	72
8-6.2.5	Document Security Specifications	72
8-6.2.6	Develop Security Plan	72
8-6.2.7	Develop or Acquire Security Controls	72
8-6.2.8	Harden Information Resources	72
8-6.2.9	Develop Application Disaster Recovery Plan	73
8-6.2.10	Develop Facility Recovery Plan	73

8-6.2.11	Develop Standard Operating Procedures	73
8-6.2.12	Incorporate Security Requirements in SLAs and Trading Partner Agreements	73
8-6.2.13	Develop Operational Security Training	73
8-6.2.14	Register Application in eAccess	73
8-6.3	Phase 3 — Testing	73
8-6.3.1	Develop Security Test Plan	73
8-6.3.2	Conduct Operational Security Training	74
8-6.3.3	Conduct Security Code Review	74
8-6.3.4	Conduct Vulnerability Scan	74
8-6.3.5	Conduct Independent Risk Assessment	74
8-6.3.6	Conduct Independent Security Code Review	74
8-6.3.6.1	Independent Security Code Review Description	74
8-6.3.6.2	Criteria for Conducting an Independent Security Code Review	74
8-6.3.7	Conduct Security Testing and Document Results	75
8-6.3.8	Conduct Independent Penetration Testing and Vulnerability Scans	75
8-6.3.8.1	Independent Penetration Testing and Vulnerability Scans Description	75
8-6.3.8.2	Criteria for Conducting Independent Penetration Testing and Vulnerability Scans	75
8-6.3.9	Conduct Independent Validation of Security Testing	76
8-6.3.9.1	Independent Validation of Security Testing Description	76
8-6.3.9.2	Criteria for Conducting Independent Validation of Security Testing	76
8-6.3.10	Address Outstanding Issues	76
8-6.4	Phase 4 — Evaluation	76
8-6.4.1	Develop ISA Documentation Package	77
8-6.4.2	Review ISA Documentation Package and Write Evaluation Report	77
8-6.4.3	Escalate Security Concerns or Certify Application	77
8-6.4.4	Escalate Security Concerns or Prepare Risk Mitigation Plan	77
8-6.4.5	Escalate Security Concerns or Accredite Application	78
8-6.4.6	Make Decision to Deploy (or Continue to Deploy) or Return for Rework	78
8-6.4.7	Deploy Application	78
8-6.5	Phase 5 — Production	78
8-6.5.1	Application Maintenance	78
8-6.5.2	Follow Security-Related Plans and Continually Monitor Operations	78
8-6.5.3	Periodically Review, Test, and Audit	78
8-6.5.4	Re-assess Risks and Upgrade Security Controls	79
8-6.5.5	Update Security-Related Plans	79
8-6.5.6	Re-initiate ISA	79
8-6.5.7	Retain ISA Documentation	79
8-6.5.8	Retire Information Resource	80

Contents

- 8-6.5.8.1 Disposal of Data 80
- 8-6.5.8.2 Sanitize Equipment and Media 80
- 8-7 Business Partnerships and Alliances 80
 - 8-7.1 Policy Compliance 80
 - 8-7.2 ISA Requirement 80
 - 8-7.3 Contractual Terms and Conditions 80
- 9 Information Security Services 81**
 - 9-1 Policy 81
 - 9-2 Roles and Responsibilities 81
 - 9-2.1 Chief Information Officer/Vice President, Information Technology 81
 - 9-2.2 Manager, Corporate Information Security Office 81
 - 9-2.3 Managers, Computing Operations/Infrastructures 82
 - 9-2.4 Manager, Secure Infrastructure Services 82
 - 9-2.5 Executive Sponsors 83
 - 9-2.6 All Managers 83
 - 9-2.7 System Administrators 84
 - 9-2.8 Database Administrators 84
 - 9-2.9 All Personnel 85
 - 9-2.10 Inspector General 85
 - 9-3 Security Services Overview 86
 - 9-4 Authorization 87
 - 9-4.1 Authorization Principles 87
 - 9-4.1.1 Clearances 87
 - 9-4.1.2 Need to Know 87
 - 9-4.1.3 Separation of Duties 87
 - 9-4.1.4 Least Privilege 87
 - 9-4.2 Authorization Process 88
 - 9-4.2.1 Baseline Information Services 88
 - 9-4.2.2 Requesting Authorization 88
 - 9-4.2.3 Approving Requests 88
 - 9-4.2.4 User Registration Management 88
 - 9-4.2.5 Periodic Review of Access Authorization 89
 - 9-4.2.6 Implementing Changes 89
 - 9-4.2.7 Revoking Access 89
 - 9-4.2.8 Emergency Access 89
 - 9-4.3 Authorization Requirements 90
 - 9-5 Accountability 90
 - 9-5.1 Description 90
 - 9-5.2 Types of Accountability 90
 - 9-5.2.1 Site Accountability 91

9-5.2.2	Network Accountability	91
9-5.2.3	Individual Accountability	91
9-5.3	Types of Accounts	91
9-5.3.1	Regular Accounts	91
9-5.3.2	Privileged Accounts	92
9-5.3.3	Managed Accounts	92
9-5.3.3.1	Shared Accounts	92
9-5.3.3.2	Training Accounts	92
9-5.3.3.3	Machine Accounts	92
9-5.3.4	Generic Accounts	93
9-5.3.5	Guest Accounts	93
9-5.3.6	Other Accounts	93
9-5.4	Account Management	93
9-5.4.1	Establishing Accounts	93
9-5.4.2	Documenting Account Information	93
9-5.4.3	Configuring Account Time-outs	93
9-5.4.4	Departing Personnel	93
9-5.5	Handling Compromised Accounts	94
9-6	Identification	94
9-6.1	Issuing Logon IDs	94
9-6.2	Protecting Logon IDs	94
9-6.3	Suspending Logon IDs	94
9-6.4	Failed Logon Attempts	94
9-6.4.1	Recording Failed Logon Attempts	94
9-6.4.2	User Notification of Failed Logon Attempt	95
9-6.5	Terminating Logon IDs	95
9-6.6	Identification Requirements	95
9-7	Authentication	95
9-7.1	Passwords	96
9-7.1.1	Password Selection Requirements	96
9-7.1.2	Password Selection Recommendations	96
9-7.1.3	Initial Password	97
9-7.1.4	Password Suspension	97
9-7.1.5	Re-set Passwords	97
9-7.1.6	Password Expiration	97
9-7.1.7	Requests for Use of Non-Expiring Password Accounts	98
9-7.1.8	Password Protection	98
9-7.1.9	Password Storage	98
9-7.1.10	Vendor Default Passwords	98
9-7.1.11	Password Requirements	99

Contents

9-7.2	Personal Identification Numbers	99
9-7.2.1	PIN Generation and Selection	99
9-7.2.2	PIN Distribution	99
9-7.2.3	PIN Protection	99
9-7.2.4	Forgotten PINs	100
9-7.2.5	PIN Suspension	100
9-7.2.6	PIN Cancellation and Destruction	100
9-7.2.7	PINs Used for Financial Transactions	100
9-7.3	Shared Secret	100
9-7.4	Digital Certificates and Signatures	101
9-7.4.1	Digital Certificates	101
9-7.4.2	Digital Signatures	101
9-7.4.3	Certificate and Signature Standards	101
9-7.5	Smart Cards and Tokens	101
9-7.6	Biometrics	101
9-7.7	Nonrepudiation and Strong Authentication	102
9-7.7.1	Nonrepudiation	102
9-7.7.2	Information Resource Nonrepudiation Requirements	102
9-7.7.3	Strong Authentication	102
9-7.8	Remote Access Authentication	102
9-7.9	Session Management	102
9-7.9.1	Session Establishment	103
9-7.9.2	Session Expiration	103
9-7.9.3	Time-out Requirements (Re-authentication)	103
9-7.9.3.1	Workstations	104
9-7.9.3.2	Applications	104
9-7.9.3.3	Remote Access	104
9-7.9.4	Failed Access Attempts	104
9-7.10	Authentication Requirements	104
9-8	Confidentiality	105
9-8.1	Description	105
9-8.2	Encryption	105
9-8.2.1	Required for Transmission and Storage on Removable Devices and Media	105
9-8.2.2	Recommended for Storage on Non-Removable Devices	105
9-8.3	Utilization of Encryption Products	106
9-8.4	Key Management	106
9-8.4.1	Protecting Encryption Keys	106
9-8.4.2	Recommended Practices	106
9-8.4.3	Key Management Requirements	107
9-8.5	Elimination of Residual Data	107

9-9	Integrity	107
9-9.1	Information Resource Integrity	107
9-9.2	Data Integrity	108
9-10	Availability	108
9-10.1	Capacity Planning and Scalability	109
9-10.2	Redundancy	109
9-10.3	Secure Backup and Recovery	109
9-10.4	High Availability	109
9-11	Security Administration	110
9-11.1	Security Administration Requirements	110
9-11.2	Security Administration Documentation Requirements	110
9-12	Audit Logging	111
9-12.1	Audit Logging Functionality Requirements	111
9-12.2	Audit Log Events	112
9-12.3	Audit Log Contents	112
9-12.4	Audit Log Protection	112
9-12.5	Audit Log Reviews	113
9-12.6	Audit Log Retention	113
10	Hardware and Software Security	115
10-1	Policy	115
10-2	Roles and Responsibilities	115
10-2.1	Chief Inspector	115
10-2.2	Manager, Corporate Information Security Office	116
10-2.3	Managers, Computing Operations/Infrastructures	116
10-2.4	Manager, Secure Infrastructure Services	116
10-2.5	Executive Sponsors	117
10-2.6	Installation Heads	117
10-2.7	System Administrators	117
10-2.8	Database Administrators	118
10-2.9	All Personnel	118
10-2.10	Inspector General	118
10-3	General Guidelines for Hardware and Software	119
10-3.1	Securing the Postal Service Computing Infrastructure	119
10-3.2	Using Approved Hardware and Software	119
10-3.3	Testing of Hardware and Software	120
10-3.4	Tracking Hardware and Software Vulnerabilities	120
10-3.5	Maintaining Inventory	120
10-3.6	Licensing Hardware and Software	120
10-3.7	Using Diagnostic Hardware and Software	120
10-4	Configuration and Change Management	120

Contents

10-4.1	Scope	120
10-4.2	Configuration Control	121
10-4.3	Standard Configurations	121
10-4.4	Change/Version Control	121
10-4.5	Patch Management	121
10-4.6	Significant Changes	122
10-4.6.1	Computing Platform	122
10-4.6.2	Application	122
10-4.7	Change Management for Pilots and Proofs of Concept	123
10-5	Hardware Security	123
10-5.1	Mainframes	123
10-5.2	Network Devices	123
10-5.3	Servers	123
10-5.3.1	Hardening Servers	123
10-5.3.2	Using Web Servers	124
10-5.3.3	Using Database Servers	124
10-5.3.4	Combined Web and Database Servers	124
10-5.4	Hardening Servers	124
10-5.4.1	Physical Security	125
10-5.4.2	Password- or Token-Protected Screen Saver	125
10-5.5	Portable Devices	125
10-6	Software and Applications Security	125
10-6.1	Software Safeguards	126
10-6.2	Secure Transaction Compliance	126
10-6.2.1	Financial Requirements	126
10-6.2.2	Health Insurance Portability and Accountability Act Requirements	126
10-6.3	Version Control	126
10-6.3.1	Updating Software	126
10-6.3.2	Distributing Software	127
10-6.3.3	Prohibited Software	127
10-6.3.4	Unapproved Software	127
10-6.4	Operating Systems	127
10-6.5	Application Software	127
10-6.6	Database Management Systems	127
10-6.6.1	DBMS Activity Logs	127
10-6.6.2	DBMS Security Features and Views	128
10-6.7	COTS Software	128
10-6.8	COTS Vulnerability Assessment	128
10-6.9	Independent Code Review	128
10-6.10	Browser Software	128
10-6.11	Third-Party Software	128

10-6.11.1	Ownership	129
10-6.11.2	Licensing and Escrow of Custom-Built Applications	129
10-6.11.3	Assurance of Integrity	129
10-7	Protection against Viruses and Malicious Code	129
10-7.1	Virus Protection Software	129
10-7.1.1	Installation	129
10-7.1.2	Scanning	129
10-7.1.3	Updating	129
10-7.2	Other Protection Measures	130
10-7.2.1	Protecting Shared and Retrieved Files	130
10-7.2.2	Evaluating Active Content or CGI Code	130
10-7.2.3	Protecting Applications	130
10-7.2.4	Creating Backups before Installation	130
10-7.2.5	Checking for Viruses before Distribution	130
10-7.2.6	Spyware Protection Measures	130
10-8	Audit Logs	131
10-8.1	General Guidelines	131
10-8.2	Protection of Audit Logs	131
10-8.3	Retention of Audit Logs	131
10-8.4	Review of Audit Logs	131
10-8.5	Operating System Audit Logs	131
10-8.6	Application Audit Logs	131
11	Networks and Communications	133
11-1	Policy	133
11-2	Roles and Responsibilities	133
11-2.1	Inspector General	133
11-2.2	Chief Inspector	133
11-2.3	Manager, Corporate Information Security Office	134
11-2.4	Manager, Secure Infrastructure Services	134
11-2.5	Manager, Information Security Services	135
11-2.6	Executive Sponsors	136
11-2.7	Installation Heads	136
11-2.8	Network Connectivity Review Board	136
11-2.9	Manager, SIS Threat Assessment and Response	137
11-2.10	System Administrators	137
11-2.11	Business Partners	138
11-2.12	All Personnel	138
11-3	Networks and Communications Security	140
11-3.1	Purpose	140
11-3.2	Scope	140

Contents

11-4	Network Architecture	140
11-4.1	Managing Network Addressing	141
11-4.2	Approving Services and Protocols	141
11-4.3	Securing Network Perimeters	142
11-4.4	Implementing Network Integrity Controls	142
11-5	Protecting the Network Infrastructure	142
11-5.1	Scope	142
11-5.2	Ensuring Physical Security	143
11-5.3	Maintaining Network Asset Control	143
11-5.4	Protecting Network Configuration Information	143
11-5.5	Implementing Identification and Authentication	143
11-5.6	Implementing Authorization	143
11-5.7	Implementing Hardening Standards	143
11-5.8	Determining When a Secure Enclave Is Required	143
11-5.9	Establishing Secure Enclaves	144
11-5.10	Isolation of Postal Service and Non-Postal Service Networks	144
11-5.11	Scanning, Penetration Testing, and Vulnerability Assessments	144
11-5.11.1	Conducting Intrusion Detection	144
11-5.11.2	Conducting Penetration Testing	145
11-5.11.3	Conducting Vulnerability Scans	145
11-6	Internet Technologies	145
11-6.1	Internet	145
11-6.2	Intranet	145
11-6.3	Extranet	145
11-7	Protecting the Network/Internet Perimeter	146
11-7.1	Implementing Internet Security Requirements	146
11-7.2	Implementing Firewalls	146
11-7.2.1	Firewall Configurations	146
11-7.2.2	Firewall Administrators	147
11-7.2.3	Firewall Administration	147
11-7.2.4	Firewall System Integrity	147
11-7.2.5	Firewall Backup	147
11-7.3	Establishing Demilitarized Zones	147
11-7.4	Monitoring Network Traffic	148
11-8	Network Connections	148
11-8.1	Establishing Network Connections	148
11-8.2	Requesting Connections	148
11-8.3	Approving Connections	148
11-9	Business Partner Requirements	148
11-10	Limiting Third-Party Network Services	148
11-11	Implementing Access and Administrative Controls	149

11-12	Remote Access	149
11-12.1	Authentication	149
11-12.2	Virtual Private Network	149
11-12.3	Modem Access	150
11-12.3.1	General Modem Access	150
11-12.3.2	Requirements for Workstations with Modems	150
11-12.4	Dial-in Access	150
11-12.5	Telecommuting	150
11-12.6	Remote Management and Maintenance	151
11-13	Network Audit Logs	151
11-13.1	General Guidelines for Network Audit Logs	151
11-13.2	Protection of Network Audit Logs	151
11-13.3	Retention of Network Audit Logs	151
11-13.4	Review of Network Audit Logs	151
11-13.5	Network and Secure Enclave Audit Logs	151
12	Business Continuity Management	153
12-1	Policy	153
12-1.1	Scope	153
12-1.2	What BCM Comprises	153
12-2	Roles and Responsibilities	154
12-2.1	Chief Inspector	154
12-2.2	Vice President, Emergency Preparedness	154
12-2.3	Vice President, Chief Technology Officer	154
12-2.4	Manager, Corporate Information Security Office	154
12-2.5	Manager, Business Continuity Management	154
12-2.6	Managers of Major Information Technology Sites	155
12-2.7	Manager, Telecommunications Services	155
12-2.8	Managers of Development Centers	155
12-2.9	Information Systems Security Officers	156
12-2.10	Portfolio Managers	156
12-2.11	Executive Sponsors	156
12-2.12	All Managers	156
12-3	Business Continuity Management	158
12-4	Business Continuity Planning	158
12-4.1	Scope	158
12-4.2	Business Continuity Planning Software	158
12-4.3	Business Continuity Plan Requirements	158
12-4.4	Business Continuity Plans	159
12-4.4.1	Incident Management Team Plan	159
12-4.4.2	Facility Recovery Plan	159

Contents

12-4.4.3	Workgroup Recovery Plan	159
12-5	Disaster Recovery Planning	160
12-5.1	Scope	160
12-5.2	Application Disaster Recovery Plan	160
12-5.2.1	Application Disaster Recovery Plan Templates	160
12-5.2.2	Application Disaster Recovery Plan Requirements	161
12-6	Relationship of Criticality, Recovery Time Objective, and Recovery Point Objective	161
12-7	Mainframe Recovery Testing for Computer Operations Service Centers	161
12-8	Backup of Information Resources	162
12-8.1	What to Back Up	162
12-8.2	Backup Schedules	162
12-8.3	Backup Inventory	162
12-8.4	Backup Storage Requirements	162
12-8.5	Off-Site Backup Storage Requirements	162
12-8.6	Backup Verification	162
12-8.7	Backup Disposal	163
12-9	BCM Plan Maintenance and Testing Requirements Summary	163
12-10	Operational Workarounds	163
12-11	Continuity of Operations Planning	164
13	Incident Management	165
13-1	Policy	165
13-2	Roles and Responsibilities	165
13-2.1	Inspector General	165
13-2.2	Manager, Office of the Inspector General, Computer Crimes Unit	165
13-2.3	Chief Inspector	166
13-2.4	Manager, Corporate Information Security Office	166
13-2.5	Managers Responsible for Computing Operations and the Advanced Computing Environment Infrastructure	166
13-2.6	Program Manager, Secure Infrastructure Services	167
13-2.7	Computer Incident Response Team	167
13-2.8	Manager, Telecommunications Services	168
13-2.9	Executive Sponsors	168
13-2.10	All Managers	168
13-2.11	Security Control Officers	169
13-2.12	System Administrators	169
13-2.13	Managers, Help Desks	170
13-2.14	All Personnel	170
13-2.15	Business Partners	170
13-3	Information Security Incidents	171

13-3.1	Overview	171
13-3.2	Reportable Incidents	171
13-4	Incident Prevention	173
13-5	Preliminary CIRT Activities	173
13-6	Incident Response	174
13-6.1	Incident Reporting	174
13-6.2	Information Resource Protection	174
13-6.3	Incident Containment	175
13-6.4	Processing Incident Reports	175
13-6.5	Incident Investigation	175
13-6.6	Incident Analysis	175
13-6.7	Incident Escalation	176
14	Compliance and Monitoring	177
14-1	Policy	177
14-2	Roles and Responsibilities	177
14-2.1	Inspector General	177
14-2.2	Manager, Office of the Inspector General Computer Intrusion Unit	177
14-2.3	Chief Inspector	178
14-2.4	Manager, Corporate Information Security Office	178
14-2.5	Chief Privacy Officer	178
14-2.6	Manager, Secure Infrastructure Services	179
14-2.7	Managers, Computing Operations/Infrastructures	179
14-2.8	All Managers	179
14-2.9	System Administrators	179
14-3	Compliance	180
14-4	Testing Security Systems and Processes	180
14-5	Inspections, Reviews, and Evaluations	181
14-5.1	Requirement	181
14-5.2	Information Resources	181
14-5.3	Facilities	181
14-6	Monitoring	182
14-6.1	General Monitoring Activities	182
14-6.2	User Agreement to Monitoring	182
14-6.3	Internet Privacy Policy Statement	182
14-6.4	User Monitoring Notification	183
14-6.5	Warning Banner	183
14-6.6	What is Monitored	184
14-6.6.1	Requesting User Monitoring	184
14-6.6.2	Approving User Monitoring	184
14-6.7	Infrastructure Monitoring	185

Contents

- 14-6.8 Intrusion Detection 185
- 14-7 Audits 185
 - 14-7.1 Description 185
 - 14-7.2 Conducting Audits 185
 - 14-7.3 Responding to Audits 185
- 14-8 Confiscation and Removal of Information Resources 186
- 15 Wireless Networking 187**
 - 15-1 Policy 187
 - 15-2 Roles and Responsibilities 187
 - 15-2.1 Corporate Information Security Office, Information Technology 187
 - 15-2.2 Manager, Telecommunications Services, IT 188
 - 15-2.3 Manager, Distributed Computing Environment, IT 188
 - 15-2.4 Executive Sponsors 188
 - 15-2.5 Installation Heads 189
 - 15-2.6 Portfolio Managers, IT 189
 - 15-2.7 Manager, Engineering Software Management, Engineering 189
 - 15-2.8 Manager, Maintenance Policies and Procedures, Engineering 190
 - 15-2.9 All Managers 190
 - 15-2.10 Information Systems Security Officers, IT 190
 - 15-3 Scope 190
 - 15-4 Baseline Requirements 191
 - 15-5 Prevention of Unacceptable Risk 191
 - 15-6 Wireless Solutions 191
 - 15-6.1 General 191
 - 15-6.2 Standard Wireless Solution 192
 - 15-6.2.1 General Requirements 192
 - 15-6.2.2 Architecture Requirements 192
 - 15-6.2.3 How to Request Standard Wireless Services 193
 - 15-6.3 Nonstandard Wireless Solution 193
 - 15-6.4 Bluetooth and Personal Area Network Applications 194
 - 15-7 Device Support 195
 - 15-8 Procurement Requirements 195
 - 15-9 Deployment Requirements 197
 - 15-9.1 Administrative Security Requirements 197
 - 15-9.2 Physical Security Requirements 198
 - 15-9.3 Technical Security Requirements 199
 - 15-9.4 Maintenance Security Requirements 200
 - 15-9.5 Security Requirements for Using a Public Hot Spot 201
 - 15-10 Compliance and Monitoring Requirements 201

Appendix A — Consolidated Roles and Responsibilities 203

Appendix B — Related Information Security Documents 231

Exhibits

Exhibit 1.3.1	
Examples of Information Resources	3
Exhibit 2.2	
Chapters Containing Role-Related Information Security Responsibilities and Activities	8
Exhibit 3.2	
Information Designation and Control Responsibilities	14
Exhibit 3.4.2	
Information Designation and Security Requirements Process	16
Exhibit 4.2	
Risk Management Responsibilities	27
Exhibit 5.2	
Acceptable Use Responsibilities	35
Exhibit 6.2	
Personnel Security Responsibilities	45
Exhibit 7.2	
Physical and Environmental Security Responsibilities	54
Exhibit 8.2	
System, Application, and Product Development Responsibilities	64
Exhibit 8.6	
Overview of ISA Process	70
Exhibit 9.2	
Security Services Responsibilities	86
Exhibit 10.2	
Hardware and Software Security Responsibilities	119
Exhibit 11.2	
Networks and Telecommunications Security Responsibilities	139
Exhibit 12.2	
Business Continuity Management Responsibilities	157
Exhibit 13.2	
Incident Management Responsibilities	171
Exhibit 14.2	
Compliance and Monitoring Responsibilities	180
Exhibit 14.5.4	
Authorized Standard Postal Service Warning Banner	184

This page intentionally left blank

1 Introduction

1-1 Policy

Handbook AS-805, *Information Security*, establishes the United States Postal Service information security policies required for appropriately identifying information resources and business requirements and appropriately protecting those information resources. 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. 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.

1-2 Purpose

The intent of this handbook and information security policies is to 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.
- 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.

1-3 Scope of Information Security Policies

1-3.1 **Information Resources**

These policies apply to all information, in any form, related to Postal Service business activities, employees, or customers, which has been created, acquired, or disseminated using Postal Service resources, brand, or funding. These policies also apply to all technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information. These 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.

For the purpose of these policies, information technologies and the information they contain are collectively known as **information resources** (see [Exhibit 1.3.1](#), *Examples of Information Resources*).

Note: The Office of the Inspector General and the Inspection Service have the autonomy to manage their own networks and information technology (IT) infrastructures.

1-3.2 **Organizations and Personnel**

These 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. These policies also apply to the Office of the Inspector General (OIG) 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.

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.

Exhibit 1.3.1

Examples of Information Resources

Category	Description	Examples	
Systems and equipment	All multi-user computers and computer-controlled systems and their components	<ul style="list-style-type: none"> ▪ Data processing equipment ▪ Automated information systems (AIS) ▪ Process control computers ▪ Process control systems ▪ Embedded computer systems ▪ Mainframe computers ▪ Minicomputers ▪ Microcomputers 	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Bar code sorters ▪ Flat sorters ▪ Optical character readers ▪ Data Collection System ▪ Intrusion Detection System 	<ul style="list-style-type: none"> ▪ Tray Management System ▪ Forwarding Control System ▪ National Directory Support System
Single-user computer equipment	All computers and their components used by individuals	<ul style="list-style-type: none"> ▪ Personal computers (PCs) ▪ Workstations ▪ Laptop computers ▪ Notebook computers 	<ul style="list-style-type: none"> ▪ Personal digital assistants (PDAs) ▪ Palm tops ▪ Handheld computers
Hardware	All major items of equipment or their components associated with a computer system	<ul style="list-style-type: none"> ▪ Central processing units (CPUs) ▪ Terminals ▪ Monitors ▪ Speakers 	<ul style="list-style-type: none"> ▪ Video display terminals ▪ Projection equipment ▪ Modems ▪ Printers
Software	All programs, scripts, applications, operating systems, HTML, and related resources	<ul style="list-style-type: none"> ▪ Operating systems ▪ Programs ▪ Applications ▪ Applets 	<ul style="list-style-type: none"> ▪ Database management systems ▪ Custom code ▪ Associated documentation
Data and information	All information or data stored in digital format, or as a printed product of data stored in digital format	<ul style="list-style-type: none"> ▪ Text files ▪ Documents ▪ Spreadsheets ▪ Digital images 	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Information delivery services ▪ E-commerce applications 	<ul style="list-style-type: none"> ▪ Digital certificate services ▪ Web site content
Network facilities	All communications lines and associated interconnected communications equipment	<ul style="list-style-type: none"> ▪ Transmission lines ▪ Terminal equipment ▪ Routers ▪ Firewalls ▪ Hubs ▪ Switches ▪ Local area networks (LANs) ▪ Wide area networks (WANs) ▪ Virtual private networks (VPNs) ▪ Infrastructure 	<ul style="list-style-type: none"> ▪ Internet ▪ Intranet ▪ Extranet ▪ Telephones and telephone systems ▪ Voice-messaging systems ▪ Fax machines ▪ Videoconferencing equipment ▪ Wireless communications
Media	All electronic and nonelectronic media used for information exchange	<ul style="list-style-type: none"> ▪ Magnetic tapes ▪ Magnetic or optical disks 	<ul style="list-style-type: none"> ▪ Diskettes ▪ Hard-copy printouts

1-4 Guiding Principles

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

Information is:

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

Information security is:

- A 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.

1-5 Importance of Compliance

1-5.1 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.

1-5.2 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.

1-5.3 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.

1-5.4 **Abiding by Federal Regulations**

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

1-6 **Information Security and the Privacy Act**

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 regarding 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.

1-7 **Information Security Program**

The chief inspector has delegated the authority for the information security program to the chief information officer/vice president, Information Technology (CIO/VP IT), who, in turn, has delegated this authority to the manager, Corporate Information Security Office (CISO). The CISO directs the Postal Service information security program, which consists of the subprograms listed below (see *Administrative Support Manual [ASM] 87* for a brief description of each subprogram):

- a. Information Security Policies, Procedures, and Standards.
- b. Risk Management.
- c. Information Security Awareness.
- d. Information Security Assurance.
- e. Information Security Technology Assessment.
- f. Security Architecture.
- g. Network Security.
- h. Business Continuity and Contingency Planning.
- i. Information Security Incident Management.
- j. Compliance.

This page intentionally left blank

2 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. Security-related roles and responsibilities must be identified and separation of duties and responsibilities considered when defining roles. Access to information resources will be based on the individual's roles and responsibilities. Only authorized personnel will be approved for access to Postal Service information resources.

2-2 How Roles and Responsibilities Are Presented

This handbook contains the roles and responsibilities associated with implementing information security. The roles and responsibilities are organized as follows:

a. High-Level Roles and Responsibilities

This chapter contains the Postal Service roles and responsibilities for individuals authorized to develop and implement the information security program. Also included are the high-level responsibilities for officers, managers, and all personnel. [Exhibit 2.2, Chapters Containing Role-Related Information Security Responsibilities and Activities](#), points to the chapters where role-related responsibilities and activities are explained in detail.

b. Roles and Responsibilities in Detail

Chapters 3 through 14 identify the roles, detailed responsibilities, and information security activities related to the information security policy described in each chapter.

c. Consolidated Roles and Responsibilities

Appendix A consolidates all of the roles and responsibilities.

Exhibit 2.2

Chapters Containing Role-Related Information Security Responsibilities and Activities

ROLES	CHAPTERS											
	3	4	5	6	7	8	9	10	11	12	13	14
Chief Inspector		X		X	X	X	X				X	X
Chief Information Officer/VP Information Technology (CIO/VP IT)	X	X				X	X	X	X			
Manager, Corporate Information Security Office (CISO)	X	X	X	X	X	X	X	X	X	X	X	X
Vice Presidents, Functional Business Areas		X				X						
All Officers, Executives, and Managers			X	X			X			X	X	X
Executive Sponsors	X	X	X			X	X	X	X	X	X	
Portfolio/Business Managers	X	X				X				X		
Accreditors						X						
Installation Heads		X			X			X	X	X		
Chief Privacy Officer (CPO)	X		X									X
Inspector General (OIG)	X	X	X	X	X	X	X		X	X	X	X
Manager, OIG Computer Intrusion Unit											X	
Manager, Information Security Services (ISS)						X			X			
Managers, Computing Operations/Infrastructures							X	X			X	X
Manager, Secure Infrastructure Services (SIS)							X		X		X	X
Manager, SIS Connectivity											X	
Network Connectivity Review Board (NCRB)									X			
Manager, SIS Threat Assessment and Response									X		X	
Managers, Help Desks											X	
Contracting Officers				X	X	X						
Business Partners						X			X		X	
Security Control Officers (SCOs)					X						X	
Information Systems Security Officers (ISSOs)	X	X				X				X		
Information Systems Security Representatives (ISSRs)	X	X				X						
Project Managers						X						
System Administrators							X	X	X		X	X
Database Administrators							X	X				
All Personnel	X		X	X	X		X	X	X		X	

2-3 Roles and Responsibilities Summary

2-3.1 Chief Inspector

The chief inspector is the security officer for the Postal Service and has delegated authority for the information security program to the chief information officer/vice president, Information Technology. (For descriptions of Postal Inspection Service responsibilities relating to security, see ASM 27.)

2-3.2 Chief Information Officer/Vice President, Information Technology

The chief information officer/vice president, Information Technology (CIO/VP IT), is responsible for ensuring the secure implementation of the information technology infrastructure and has delegated authority for development, implementation, and management of the Postal Service information security program to the manager, Corporate Information Security Office (CISO). The CIO/VP IT is also responsible for information assurance.

2-3.3 Manager, Corporate Information Security Office

The manager, CISO, is responsible for setting the overall strategic and operational direction of the information security program and its implementation strategies, including the development of information security policies and processes, and for directing the Corporate Information Security Office in Washington, DC, and Information Security Services (ISS) in Raleigh, NC. The manager, CISO, serves as the central point of contact for all information security issues; provides overall consultation and advice on information security policies, processes, requirements, controls, services, security awareness training, and issues; and assesses and ensures compliance with information security policies through inspections, reviews, and evaluations.

2-3.4 Chief Privacy Officer

The chief privacy officer is responsible for developing privacy policy and compliance standards, determining information sensitivity, managing the Postal Service records organization, and providing guidance related to privacy policy.

2-3.5 Inspector General

The inspector general, Office of the Inspector General (OIG), is responsible for investigating, evaluating, and auditing programs and operations of the Postal Service to ensure the efficiency and integrity of the postal system and to ensure that its assets and resources are fully protected. These responsibilities are based on the OIG/Inspection Service *Designation of Functions* as approved by the Postal Service Board of Governors.

2-3.6 **Technology Managers**

All 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.

2-3.7 **All Officers and Managers**

All officers, business and line managers, and supervisors, regardless of functional area, are responsible for implementing information security policies. All officers and managers 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.

2-3.8 **All Personnel**

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

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 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. These information resources belong to the Postal Service as an organization and not to any individual or group of individuals. Postal Service information resources must comply with Postal Service policies and procedures on data stewardship.

3-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for information designation and control are defined in the sections below and are depicted in [Exhibit 3.2](#).

3-2.1 Executive Sponsors

Executive sponsors are the business managers with oversight (funding, development, production, and maintenance) of the information resource and are responsible for the following:

- a. Consulting with the chief privacy officer (CPO) on determining information sensitivity and Privacy Act applicability.
- b. Completing the business impact assessment (BIA) to determine the sensitivity and criticality of each information resource under his or her control, assess potential consequences of information resource unavailability, and identify security requirements to appropriately protect the information resource.
- c. Appointing, in writing, an information systems security representative (ISSR).
- d. Providing financial and personnel resources to complete the BIA.

3-2.2 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Developing policy regarding the determination of criticality and the appropriate security requirements to protect the information resource.
- b. Providing overall consultation and advice relative to the BIA process and associated security requirements.
- c. Assessing and ensuring compliance with information designation and control policies through inspections, reviews, and evaluations.

3-2.3 **Chief Privacy Officer**

The chief privacy officer (CPO) is responsible for the following:

- a. Developing policy relating to the determination of information sensitivity designation.
- b. Developing policy on Postal Service privacy issues.
- c. Providing guidance to ensure Postal Service compliance with the Freedom of Information Act, Gramm-Leach-Bliley, Children's Online Privacy Protection Act, and the Privacy Act.
- d. Developing privacy compliance standards, customer privacy statement, and customer data collection standards (including cookies and web transfer notification).
- e. Developing appropriate data record retention, disposal, and release guidelines.

3-2.4 **Portfolio/Business Managers**

Portfolio/business managers are responsible for the following:

- a. Ensuring the information resource is entered in the Enterprise Information Repository (EIR), documenting the determination of sensitivity and criticality for each information resource, and updating the EIR as required.
- b. Functioning as the liaison between executive sponsors and information technology providers.
- c. Supporting the executive sponsor in the development of information resources and the business impact assessment.

3-2.5 **Information Systems Security Officers**

Information systems security officers (ISSOs) are responsible for the following:

- a. Ensuring a business impact assessment (BIA) is completed for each application system and an infrastructure impact assessment (IIA) is completed for each infrastructure component.
- b. Advising and consulting with executive sponsors and portfolio managers during the BIA and IIA processes so they know about (1)

security requirements for information resources and (2) mandatory security requirements for information resources when the resources are designated sensitive or critical.

- c. Specifying additional mandatory security requirements based on federal legislation (e.g., Children's Online Privacy Protection Act [COPPA]), federal regulation (e.g., requirements for cryptographic modules), federal directive (e.g., Homeland Security Presidential Directive [HSPD] 12, personal identity verification), industry requirement (e.g., payment card industry standards, requirements, and guidelines), the operating environment (e.g., hosted in the de-militarized zone [DMZ]), and the risks associated with the information resource.
- d. Recommending discretionary security requirements based on generally accepted industry practices to executive sponsors and portfolio managers during the BIA and IIA processes.

3-2.6 **Information Systems Security Representatives**

Information systems security representatives (ISSRs) are appointed in writing by the executive sponsors 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. ISSRs are responsible for providing support to the executive sponsor and portfolio manager as required.

3-2.7 **Project Managers**

Project managers are responsible for updating the EIR on behalf of the portfolio manager.

3-2.8 **All Personnel**

All personnel are responsible for the secure handling of information and media.

3-2.9 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 3.2

Information Designation and Control Responsibilities

Activity	Executive Sponsors	Portfolio/Business Managers & ISSRs	CISO	CPO	ISSOs	All Personnel	OIG
Conduct BIA.	X	P	C	C	C		A
Handle information and media securely.	X		C	C	C	X	A

X = Responsible for accomplishment

P = Provide assistance

C = Consulting support as required

A = Independent audits, evaluations, and reviews

(See Appendix A for a consolidated list of roles and responsibilities.)

3-3 Information Designation

3-3.1 Information Designation Categories and Levels

The Postal Service uses two information designation categories; each category has three levels. The sensitivity and criticality level designations are determined during the BIA. Designation categories and levels are as follows:

- a. Sensitivity Category/Levels. Sensitivity determines the need to protect the confidentiality and integrity of the information. The levels of sensitivity, in decreasing order of necessity to protect the confidentiality and integrity of the information, are as follows:
 - (1) Sensitive.
 - (2) Business-controlled sensitivity.
 - (3) Nonsensitive.
- b. Criticality Category/Levels. Criticality reflects the need for continuous availability of the information. The levels of criticality, in decreasing order of necessity to protect the continued availability of the information, are as follows:
 - (1) Critical.
 - (2) Business-controlled criticality.
 - (3) Noncritical.

Note: National security classified information is not addressed by this handbook. See the Inspection Service for appropriate policy regarding national security classified information.

3-3.2 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* criticality level may have *any* level of sensitivity designation and vice versa.

3-3.3 **Determination of Sensitivity and Criticality**

3-3.3.1 **Business Impact Assessment**

The BIA is a process for determining the sensitivity and criticality levels 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. A BIA is required every three years, whenever a significant change is made to the information resource, or whenever the Information Security Assurance (ISA) process is re-initiated (see 8-6.5.6, Re-initiate ISA).

3-3.3.2 **Business Impact Assessment Process**

The BIA process addresses, among other things, the disclosure and unauthorized modification of sensitive information, the unauthorized destruction or unavailability of critical information, legal and regulatory requirements, and prudent business practices. The BIA process can encompass multiple business processes or focus on one particular aspect of the business. It provides the framework for risk management and documents the following:

- a. Identification of the information resource.
- b. Distinct roles and responsibilities related to the information resource.
- c. Sensitive and business-controlled sensitivity information resources or other resources that need to be protected from disclosure or modification.
- d. Critical and business-controlled criticality information resources or other resources that need to be protected from destruction or unavailability.
- e. Possible disruptions and their impacts on the resource over time.
- f. Internal and external dependencies of the information resource.
- g. Security requirements appropriate for protection of the information resource.

3-3.3.3 **Recording Information Resource Designation**

The determination of sensitivity and criticality for each information resource must be documented in the Enterprise Information Repository (EIR), also known as the System Index.

3-4 **Security Requirements**

3-4.1 **Security Requirements and Controls**

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.

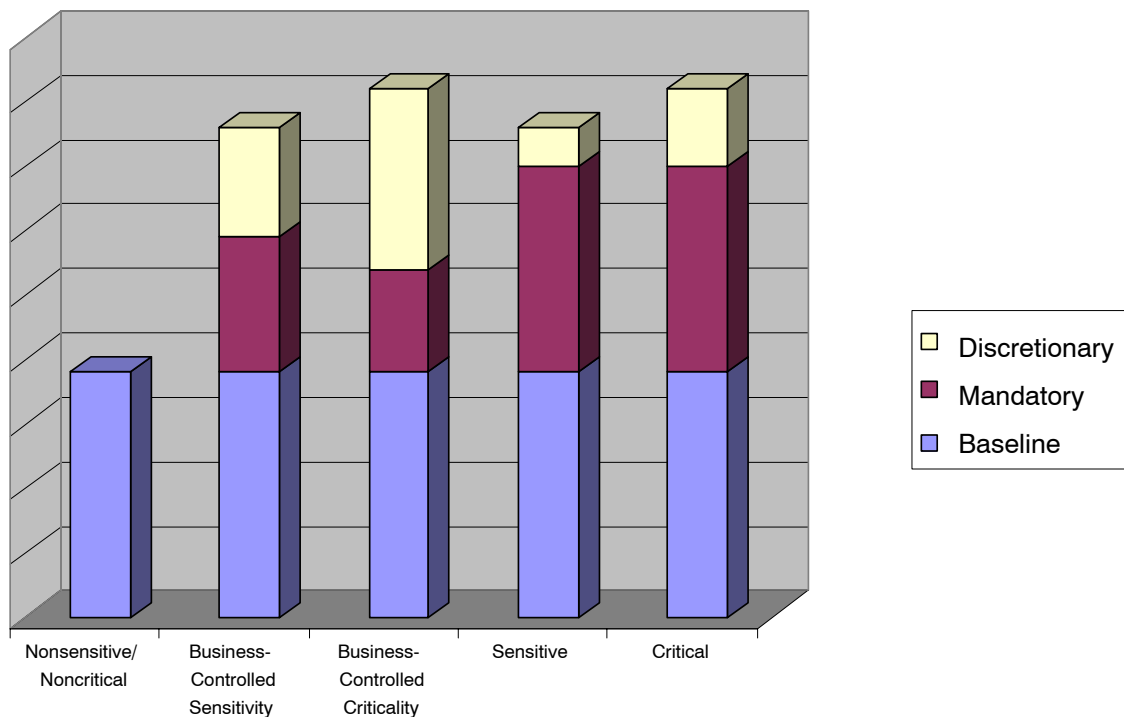
3-4.2 Security Requirement Categories

The Postal Service uses the following three categories of security requirements to protect information resources according to their sensitivity and criticality:

- a. Baseline.
- b. Mandatory.
- c. Discretionary.

[Exhibit 3.4.2](#), *Information Designation and Security Requirements Process*, reflects the types of requirements applicable to each designation.

Exhibit 3.4.2
Information Designation and Security Requirements Process



3-4.3 Baseline Security Requirements

All information resources must implement controls sufficient to satisfy the baseline security requirements. Baseline security requirements have been established to protect the postal computing environment and infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction.

3-4.4 **Mandatory Security Requirements**

Additional security will be needed to adequately protect sensitive, critical, and business-controlled information resources. Mandatory requirements are based on the following:

- a. How sensitive or critical the information resource is (determined during the BIA).
- b. Federal legislation (e.g., Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, COPPA).
- c. Federal regulations (e.g., requirements for cryptographic modules).
- d. Federal directives (e.g., personal identity verification, critical infrastructure).
- e. Industry requirements (e.g., payment card industry).
- f. Operating environment (e.g., application is hosted in the DMZ, changes in technology, changes in the Postal Service mission).
- g. Risks determined during the risk assessment process.
- h. Vulnerabilities discovered at any time during the information resource lifecycle.

If any of these additional mandatory requirements conflict with the requirements included in Handbook AS-805, the most restrictive or protective requirement applies.

3-4.5 **Discretionary Security Requirements**

ISSOs may recommend additional discretionary security requirements during the BIA and IIA processes to better protect sensitive, critical, and business-controlled information resources. Discretionary security requirements based on generally accepted industry practices are recommended. The executive sponsor assumes the risks associated with not implementing the recommended discretionary security requirements.

3-5 **Handling Information and Media**

All Postal Service information, whether in electronic or nonelectronic format, 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.

3-5.1 **Labeling of Information and Media**

3-5.1.1 **Sensitive Information**

Sensitive information included in electronic media (e.g., disks, diskettes, tapes, and USB storage devices) and hardcopy output (e.g., printouts, screen prints, photo-copies, architecture drawings, and engineering layouts) must be legibly and durably labeled as "RESTRICTED INFORMATION."

On applications processing 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 and should be properly protected from unauthorized access or disclosure.”

Caution: The “Print Screen” function can also result in hardcopy that must be legibly and durably labeled as “RESTRICTED INFORMATION.”

3-5.1.2 **Business-Controlled Sensitive Information**

Business-controlled sensitive information included in electronic media (e.g., disks, diskettes, tapes, and USB storage devices) and hardcopy output (e.g., printouts, screen prints, photocopies, architecture drawings, and engineering layouts) must be legibly and durably labeled as “RESTRICTED INFORMATION.”

On applications processing business-controlled sensitive information, the following statement must be prominently displayed on the login/password screen or the welcome screen:

“Information within this application is designated business-controlled sensitive and should be properly protected from unauthorized access or disclosure.”

3-5.2 **Controlling Access to Information**

Sensitive and business-controlled sensitive information must be protected from unauthorized access and disclosure. Access must be restricted to authorized personnel with a need to know. Metadata must also be protected from unauthorized access and disclosure.

Critical and business-controlled critical information must be protected from unauthorized access and destruction.

3-5.3 **Retention of Information**

All Postal Service information, whether in electronic or nonelectronic format, must be retained in accordance with legal retention requirements established by law and also with operational retention requirements established by the Postal Service Records Office (see Handbook AS-353).

3-5.4 **Storage of Information**

Postal Service information must not be stored on non-Postal Service-owned devices. Postal Service information not available to the public must not be commingled with information that does not belong to the Postal Service.

3-5.4.1 **Sensitive Information**

Sensitive information, whether in electronic or non-electronic format, must be stored in a controlled area or a locked cabinet in accordance with established Postal Service policies and procedures (see Handbook AS-353).

3-5.4.2 **Business-Controlled Sensitive, Critical, and Business-Controlled Critical Information**

Business-controlled sensitive, critical, and business-controlled critical information, whether in electronic or non-electronic format, must be stored in a controlled area or a locked cabinet in accordance with established Postal Service policies and procedures (see Handbook AS-353).

3-5.4.3 **Isolation of Postal Service and Non-Postal Service Information**

Non-publicly available Postal Service information must be isolated from non-Postal Service information (e.g., business partner and vendor information) unless required by law or regulation. Non-publicly available Postal Service and non-Postal Service information must not be commingled in storage at Postal Service facilities, non-Postal Service facilities, or at backup sites unless required by law or regulation.

3-5.5 **Encryption of Information**

3-5.5.1 **Encryption of Information in Transit Across Networks**

Sensitive and business-controlled sensitive information must be encrypted in transit across networks.

3-5.5.2 **Encryption of Information on Removable Devices or Media and in Offsite Storage**

Sensitive and business-controlled sensitive information stored or archived on removable devices or media including disks, diskettes, CDs, and USB storage devices must be encrypted. Sensitive and business-controlled sensitive information that is stored off Postal Service premises must also be encrypted.

3-5.5.3 **Encryption of Payment Card Industry Information**

Payment card industry (PCI) information must be encrypted throughout the lifecycle.

3-5.6 **Removal of Postal Service Information from Postal Service Premises**

The requirements for (1) accessing or downloading sensitive and business-controlled sensitive Postal Service electronic information off Postal Service premises or (2) taking sensitive and business-controlled sensitive Postal Service electronic and non-electronic 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 and business-controlled sensitive Postal Service electronic information from Postal Service premises must be approved in writing by the functional vice president (data steward) and the Chief Information Officer (CIO).

- b. Only authorized personnel are allowed to pick up, receive, transfer, or deliver Postal Service sensitive and business-controlled sensitive information.
- c. Postal Service information accessed, processed, or stored at non-Postal Service sites must use Postal Service–owned hardware and software. The use of business partner hardware and software must be approved by the CIO and the functional vice president (data steward) and must meet Postal Service standards for server hardening and malicious code protection.
- 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 and business-controlled sensitive information must be encrypted during transmission and in storage on removable devices and media. Also all sensitive and business-controlled sensitive information must be encrypted in storage off Postal Service premises.
- f. All Postal Service hardware devices, hardcopy, and media (including backups) containing sensitive and business-controlled sensitive information must be secured against theft (e.g., personal valuables safe, gun safe, locked cabinet, locked cable). Approved business partner devices must be likewise secured.
- g. There must be accountability in the life cycle management of any sensitive and business–controlled sensitive information removed off Postal Service premises. This data and all copies must be inventoried annually and formally tracked (e.g., logbook, tape management system) from creation to destruction.

3-5.7 **Release of Information**

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

3-5.7.1 **Sensitive Information**

Sensitive information must be protected against unauthorized disclosure, whether formally or informally through conversations, email, voice, fax, and observed workstation screens.

3-5.7.2 **Business-Controlled Sensitivity Information**

It may be recommended that certain business-controlled sensitivity information be protected against unauthorized disclosure, whether formally or informally through conversations, email, voice, fax, and observed workstation screens.

3-5.7.3 **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 or business-controlled sensitivity information.

3-5.7.4 **Precautions Prior to Maintenance**

To prevent inadvertent disclosure of sensitive or business-controlled sensitivity 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 or business-controlled sensitivity 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.

3-6 Disposal and Destruction of Information and Media

3-6.1 **Disposal of Electronic Hardware and Media**

To prevent inadvertent disclosure of sensitive or business-controlled sensitivity 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.

3-6.2 **Removal of 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 and business-controlled sensitivity 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.

3-6.3 **Disposal of Nonelectronic Information**

When no longer needed, all Postal Service information designated as sensitive and business-controlled sensitivity in nonelectronic format must be destroyed by shredding, pulping, or burning (see Handbook AS-353).

3-7 **Handling Contaminated Information Resources**

3-7.1 **Sensitive and Business-Controlled Sensitive Information**

Any personnel handling contaminated Postal Service information resources must follow the guidelines set forth by the Inspection Service for handling contaminated devices. If the contaminated information resource contains sensitive or business-controlled sensitivity information, the Inspection Service must be notified regarding the type of device, the kind of data it contains (i.e., sensitive or business-controlled sensitivity), 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.

3-7.2 **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.

3-7.3 **Reporting of Contaminated Information Resources**

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

3-8 Handling Non-Postal Service Information

3-8.1 **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.

3-8.2 **National Security Classified Information**

National security classified information must not be stored, processed, or transmitted using Postal Service information resources without prior approval of the chief inspector.

This page intentionally left blank

4 Risk Management

4-1 Policy

Risk management in the Postal Service will be implemented to ensure cost-effective protection of information, applications, information resources, and the continuity of business operations. Risk assessments are required for all critical, sensitive, and business-controlled information resources, whether developed and operated in house or by business partners. Site security reviews are also required for all facilities that house critical, sensitive, and business-controlled 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.

4-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for risk management are defined in the sections below and are depicted in [Exhibit 4.2](#).

4-2.1 **Vice Presidents, Functional Business Areas**

Vice presidents of the appropriate functional business areas, together with the chief information officer/vice president, Information Technology (CIO/VP IT), are responsible for accepting residual risk of information resources.

4-2.2 **Chief Information Officer/Vice President, Information Technology**

The chief information officer/vice president, Information Technology (CIO/VP IT), together with the vice president of the appropriate functional business area, is responsible for accepting residual risk of information resources.

4-2.3 **Executive Sponsors**

Executive sponsors are the business managers with oversight (funding, development, production, and maintenance) of the information resource and are responsible for the following:

- a. Ensuring completion of an information resource risk assessment for all sensitive, critical, and business-controlled information resources under their purview.
- b. Ensuring completion of a site security review if the facility hosts a sensitive, critical, or business-controlled information resource.
- c. Providing the personnel and financial resources for risk management activities associated with information resources under their control.

4-2.4 **Portfolio/Business Managers**

Portfolio/business managers will support the executive sponsor as required.

4-2.5 **Information Systems Security Representatives**

Information systems security representatives (ISSRs) are responsible for the following:

- a. Providing support to the executive sponsor as required.
- b. Notifying the executive sponsor and ISSO of any additional security risks or concerns that emerge during development or acquisition of the information resource.

4-2.6 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Developing Postal Service policies on risk management.
- b. Providing overall consultation and advice on Postal Service risk management programs.
- c. Ensuring implementation of risk management policies and procedures.
- d. Assessing the adequacy of risk management processes in a changing information infrastructure and updating those processes as necessary.
- e. Assessing and ensuring compliance with information security risk management policies through inspections, reviews, and evaluations.

4-2.7 **Information Systems Security Officers**

Information systems security officers (ISSOs) assigned to an information resource are responsible for the following:

- a. Providing guidance on the applicability of threats or vulnerabilities.
- b. Providing guidance on the appropriate choice of countermeasures.
- c. Conducting or assisting the Inspection Service in conducting site security reviews.

4-2.8 **Installation Heads**

Installation heads of facilities that host sensitive, critical, or business-controlled information resources are responsible for the following:

- a. Ensuring completion of a site security review.
- b. Providing assistance to the Inspection Service and the ISSO in the completion of a site security review.
- c. Accepting site residual risk.

4-2.9 **Chief Inspector**

The chief inspector, Inspection Service, independently or in conjunction with the CISO, is responsible for conducting site security reviews.

4-2.10 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 4.2
Risk Management Responsibilities

Activity	CIO/VP IT & VPs, FBAs ¹	Executive Sponsors	Portfolio/ Business Managers & ISSRs	CISO	ISSOs	Installation Heads	Chief Inspector	Inspector General
Conduct information resource risk assessment.	R	X/S/F	P	C	C			A
Conduct site security review (postal facility).				C	S	X/P/R	C/S	A
Conduct site security review (nonpostal facility).	R	X/F		C	S		C/S	A

¹Chief information officer/vice president, Information Technology, and vice presidents, functional business areas

- X = Responsible for accomplishment
- P = Provide assistance
- R = Accept risk or approve additional controls
- F = Responsible for funding
- C = Consulting support as required
- S = Conduct assessments/reviews
- A = Independent audits, evaluations, and reviews

(See Appendix A for a consolidated list of roles and responsibilities.)

4-3 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.

4-4 Information Resource Risk Management

Information resource risk management is a holistic strategic and tactical approach aimed at protecting information resources by reducing their exposure to known or anticipated vulnerabilities. Risk management consists of the following major processes:

- a. Information resource risk assessment.
- b. Information resource risk mitigation.
- c. Information resource risk acceptance.
- d. Information resource risk documentation.

4-4.1 Information Resource Risk Assessment

4-4.1.1 Purpose

Risk assessment is a process that will be performed for each sensitive, critical, or business-controlled information resource to:

- 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 (or countermeasures).
- f. Analyze the costs and benefits of the safeguards in reducing the risks.
- g. Complete the information resource risk assessment report.

4-4.1.2 Frequency of Risk Assessment

A risk assessment will be performed in conjunction with system development. Additional risks may be identified as development progresses through requirements definition, design, coding, and testing.

4-4.1.3 Re-assessments

The risk assessment will be re-assessed and updated as follows:

- a. At least every three years following deployment of a resource unless earlier re-assessment is warranted.
- b. After a significant audit finding.

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

Note: The risk assessment may be re-assessed and updated after an information security incident that violates an explicit or implied security policy and compromises the integrity, availability, or confidentiality of an information resource.

4-4.2 Information Resource Risk Mitigation

Risk mitigation is 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.

4-4.3 Information Resource Risk Acceptance

Risk acceptance is the process of acknowledging that some risk exists, even after cost-effective safeguards have been implemented, and formally deciding to accept that 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.

Note: The vice president of the functional business area and the CIO/VP IT are jointly responsible for acknowledging and accepting, in writing, the risks inherent with using that information resource or initiating steps to mitigate the residual risk.

4-4.4 Information Resource Risk Management Documentation

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 Information Security Services (ISS).

4-5 Independent Risk Management

4-5.1 Independent Risk Assessment

Independent risk assessments are conducted by organizations that are separate and distinct from those responsible for the development and operation of the information resources. Such assessments will follow the independent risk assessment guidelines provided in Handbook AS-805-A, *Information Security Assurance*.

Note: Independent processes (e.g., independent risk assessment, independent code review, independent security test validation, independent penetration testing and vulnerability scans) are evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information resources. An independent process is conducted by an organization that is separate and distinct from those responsible for the development and operation of the information resource.

4-5.2 Criteria for Conducting Independent Risk Assessments

An independent risk assessment may be recommended during the business impact assessment (BIA) process when information resources are:

- a. Publicly accessible.
- b. Developed, hosted, or managed primarily by non-Postal Service personnel.
- c. Highly visible or have high impact.

Note: An independent risk assessment may be required at any time by the CIO/VP IT; manager, CISO; or vice president of the functional business area.

4-6 Site Risk Management

Site risk management consists of the following major processes:

- a. Site security review.
- b. Site risk mitigation.
- c. Site risk acceptance.
- d. Site risk documentation.

4-6.1 Site Security Review

A site security review will be performed for each site that will host sensitive, critical, or business-controlled information resources to:

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

- b. Identify the sensitive, critical, and business-controlled information resources hosted by that facility.
- c. Identify the threat events that could occur, including physical threats (power failure, fire, building collapse, water damage from plumbing failure and roof leak, etc.); environmental threats (earthquake, flooding, tornadoes, lightning, sink hole, etc.); and human threats (union lockouts, riot, disgruntled employee or customer, armed theft, etc.).
- 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.
- g. Complete the site security review report.

4-6.2 Frequency of Site Security Review

A site security review will be 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 three years, unless an earlier site security review is warranted.

4-6.3 Site Risk Mitigation

The site risk mitigation process is the same as the information resource risk mitigation process (see 4-4.2).

4-6.4 Site Risk Acceptance

Risk acceptance is acknowledging that some risk exists, even after cost-effective safeguards have been implemented, and then formally deciding to accept that risk.

Note: The installation head is responsible for acknowledging and accepting site risk. For information resources residing at non-Postal Service facilities, the vice president of the functional business area is responsible for acknowledging and accepting site risk.

4-6.5 Site Risk Management Documentation

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.

This page intentionally left blank

5 Acceptable Use

5-1 Policy

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

5-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for acceptable use are defined in the sections below and are depicted in [Exhibit 5.2](#).

5-2.1 Chief Privacy Officer

The chief privacy officer is responsible for the following:

- a. Providing guidance to ensure Postal Service compliance with the Privacy Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, and Freedom of Information Act.
- b. Developing privacy compliance standards, customer privacy statement, and customer data collection standards, including cookies and web transfer notifications.
- c. Reviewing and approving written requests for monitoring an individual's noncompliance with these acceptable use policies.

5-2.2 Executive Sponsors

Executive sponsors are responsible for the following:

- a. Informing personnel of Postal Service policies on monitoring and acceptable use of information resources.
- b. Ensuring that contract personnel under their supervision comply with Postal Service information security policies and procedures.
- c. Ensuring that all hardware and software are obtained according to official Postal Service processes.

- d. Ensuring compliance with and implementation of the Postal Service privacy policy, data collection policy, and customer privacy statement.

5-2.3 **All Managers**

Managers at all levels are responsible for the following:

- a. Informing personnel of Postal Service policies on monitoring and acceptable use of information resources.
- b. Ensuring that personnel under their supervision comply with Postal Service information security policies and procedures.
- c. Initiating written requests for monitoring an individual's noncompliance with these acceptable use policies and sending the request to the chief privacy officer (CPO) for approval.
- d. Ensuring that all hardware and software are obtained according to official Postal Service processes.
- e. Ensuring that all personnel under their direction with access to information resources receive information security training commensurate with their position and responsibilities, including policies on acceptable use of information resources.
- f. Promulgating the information security awareness program for all personnel under their direction, ensuring that personnel under their supervision comply with Postal Service information security policies and procedures, and invoking user sanctions as required.

5-2.4 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Developing acceptable use policy.
- b. Developing awareness and training materials.
- c. Assessing and ensuring compliance with information security acceptable use policies through inspections, reviews, and evaluations.

5-2.5 **All Personnel**

All personnel are responsible for the following:

- a. Abiding by Postal Service policies on acceptable use of information resources.
- b. Promptly reporting suspicion or occurrence of any unauthorized activity (see Chapter 13, Incident Management).
- c. Ensuring compliance with copyright and licensing.
- d. Using approved software and hardware.
- e. Protecting intellectual property.
- f. Complying with electronic mail policy.
- g. Complying with electronic mail encryption policy.

- h. Complying with Internet policy.
- i. Any use made of their accounts, logon IDs, passwords, PINs, and tokens.

5-2.6 Inspector General

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 5.2

Acceptable Use Responsibilities

Activity	Executive Sponsors	Officers, Executives, & Managers	CPO	CISO	All Personnel	Inspector General
Notify users regarding monitoring & acceptable use, invoke user sanctions.	X	X		X/C		A
Comply with official Postal Service processes for acquiring hardware & software.	X	X		C		A
Comply with copyright & licensing. Use approved software. Protect intellectual property. Comply with email & email encryption policy. Comply with Internet policy. Comply with information resource use policy.				C/M	X	A
Implement customer privacy statement. Comply with privacy policy statements. Comply with customer data collection policy.	X		C			A

X = Responsible for accomplishment

C = Consulting support as required

M = Compliance monitoring

A = Independent audits, evaluations, and reviews

(See Appendix A for a consolidated list of roles and responsibilities.)

5-3 Monitoring

5-3.1 Right to Monitor

The Postal Service owns and reserves the right to monitor all uses of its information resources to improve the security of and ensure appropriate use of such resources and protect the resources from attack. The Postal Service will monitor network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage. Intentional misuse of information resources will be investigated by authorized law enforcement and may result in federal prosecution.

5-3.1.1 Use Constitutes Permission

Use of information resources residing on the Postal Service Intranet or connected to the Postal Service Managed Network Services (MNS) constitutes permission to monitor that use. This applies to employees,

contractors, subcontractors, and business partners whose duties require access to conduct Postal Service business.

5-3.1.2 **Public Web Site Monitoring**

Authorized use by customers whose only access is through publicly available services, such as public web sites of the Postal Service, will only be monitored for site security purposes to ensure that information resources remain available to all users.

5-3.2 **Notification of Monitoring**

Users will be notified that Postal Service networks, computers, and workstations may be monitored and viewed by appropriate, authorized personnel regardless of privacy concerns. Where feasible, this notification will appear in a warning banner whenever a user logs on to a system. Users will also be notified of Postal Service monitoring policy during information security awareness training and published policy and procedure documents.

5-4 **Ensuring Compliance**

To ensure compliance with its information security policies, the Postal Service will monitor, inspect, and audit. The Postal Service is authorized to collect and remove any information without permission or notice. Personnel must be trained in what use is acceptable and what is prohibited. Any infraction of Postal Service acceptable use policies will constitute a security violation for which personnel will be held personally accountable and subject to disciplinary action or criminal prosecution.

5-5 **Hardware and Software**

5-5.1 **Acquiring Hardware and Software**

All hardware and software must be acquired from official Postal Service sources. Software not listed on the Infrastructure Toolkit (ITK) must be approved by the Enterprise Architecture Committee (EAC).

5-5.2 **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.

5-5.3 Using Approved Software

To protect the integrity of Postal Service information resources, only approved software may be used in the Postal Service computing environment (PCE). To obtain approval to use software not on the ITK, a formal request must be made to the EAC. The formal request process applies to: purchased and licensed applications; shareware; freeware; and downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs), and wide area networks (WANs).

Unapproved software will be removed by IT personnel.

In addition to approval by the EAC, shareware and freeware must have a formal code review performed and must be scanned for viruses and malicious code prior to use on any Postal Service information resource. Software used in Engineering initiatives associated with the MPE/MHE environment that use or interact with IT information resources must be approved by the EAC and registered on the ITK.

5-5.4 Protecting Intellectual Property

To ensure the integrity of software developed by or for the Postal Service, all personnel must abide by the intellectual property protection contract provisions of the Postal Service (see the Postal Service *Purchasing Manual*).

5-5.5 Protecting Postal Service Networks

To ensure the protection of the Postal Service infrastructure, personnel working at alternative work sites must only use Postal Service-approved computer software, hardware, 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 hardware must have the latest security patches or fixes installed, virus software approved by the Postal Service and installed with the latest pattern recognition file and, if connecting via the Internet, a firewall approved by the Postal Service must be implemented.

5-6 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. 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.

If you do not comply with the Postal Service e-mail policies defined in this section, your e-mail account may be suspended and you will have to request that your manager apply to the CIO/VP IT for re-instatement of the lost privileges.

Only authorized personnel who need to know may receive restricted information.

5-6.1 **Acceptable Use**

Occasional and incidental personal email use is permitted if it does not interfere with the Postal Service's ability to perform its mission and meets the conditions outlined in Postal Service policies and procedures. However, while they remain in the system, personal messages will be considered to be in the possession and control of the Postal Service.

5-6.2 **Prohibited Use**

Do not use Postal Service information resources to check personal email accounts, such as Hotmail, Yahoo, Excite, MSN, etc. Other prohibited activities when using Postal Service email 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 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.

5-6.3 **Encryption**

Encrypting email or messages must comply with the following:

- a. Encryption software and methods must be approved by the EAC.
- 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 email must be placed in a directory or file system that can be accessed by management prior to encrypting email.
- d. Recovery keys or other devices needed to decrypt email must be provided when requested by authorized Postal Service management, the Postal Inspection Service, or the OIG.
- e. Keys may not be escrowed in customer product offerings unless specifically requested in writing by the customer and approved by the executive sponsor.

5-6.4 **Authorized Monitoring**

System administrators and other personnel with unrestricted access to data, email, and similar services must receive management approval from the CPO or manager, CISO, prior to decrypting or reading the email traffic of other personnel (see Chapter 14, Compliance and Monitoring).

5-7 **Internet**

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.

5-7.1 **Acceptable Use**

The Postal Service provides Internet access to facilitate the conduct of Postal Service business. Occasional and incidental personal Internet use is permitted if it does not interfere with the work of personnel or the Postal Service's ability to perform its mission and meets the conditions outlined in Postal Service policies and procedures (see MI EL-660-2000-5, *Limited Personal Use of Government Office Equipment*).

5-7.2 **Prohibited Use**

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 or business-controlled sensitivity 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 and push data updates, 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).

5-8 Generally Prohibited Uses of Postal Service Information Resources

Generally prohibited activities when using Postal Service 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, Secure Infrastructure Services.
- i. Promoting or maintaining a personal or private business or using Postal Service information resources for personal gain.
- j. Using someone else's logon ID and password.
- k. 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.
- l. Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.
- m. Disclosing any Postal Service information that is not otherwise public without authorized management approval.
- n. 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.

5-9 Prohibited Uses of Personal Information Resources

Prohibited activities when using personal information resources include, but are not limited to, the following:

- a. Do not bring personal information resources (e.g., laptops, notebooks, personal digital assistants [PDAs], handheld computers, or storage media including universal serial bus [USB] port devices) into Postal Service facilities.
- b. Do not connect personal information resources to the Postal Service Intranet (Blue).
- c. Do not use imaging devices (e.g., cameras, cell phones with cameras, or watches with cameras) at Postal Service facilities except as authorized by the user's vice president or his or her designee for business purposes.

5-10 Protection of Privacy

Sensitive and business-controlled sensitive 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 (FOIA), and records management can be found in Handbook AS-353. Postal Service privacy policy for customers is posted on *www.usps.com*.

5-10.1 **Nonpublic Information Resources**

Postal Service information resources not available to the general public may include the Postal Service network, workstations, and the Postal Service Intranet. Since these resources may be monitored, all personnel and customers who access these information resources will have no expectation of privacy.

5-10.2 **Publicly Available Information Resources**

Postal Service information resources available to the general public may include Internet sites or stand-alone workstations for customer use.

5-10.3 **Tracking Devices on Web Sites**

Postal Service policy addressing tracking devices is contained in the Postal Service privacy policy on *www.usps.com*. Use of persistent tracking devices (e.g., cookies and Web beacons) must be in accordance with this policy.

5-10.4 Customer Data Collection

Customer data collection can take many forms and is strictly governed by the Postal Service privacy policy and the Privacy Act as applicable. Postal Service policy addressing customer data collection may be found on a link from *www.usps.com*.

5-10.5 Transfer to Another Site

All information resources must notify the Postal Service customer before transferring the customer to an external web site not under Postal Service control.

6 Personnel Security

6-1 Policy

The Postal Service will identify sensitive positions and ensure that individuals assigned to those positions have the appropriate level of clearance to minimize risk to Postal Service information resources. Personnel will be held accountable for carrying out their information security responsibilities. Managers will ensure personnel receive appropriate information security training and protect Postal Service resources when personnel depart under involuntary or adverse conditions.

6-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for personnel security are defined in the sections below and are depicted in [Exhibit 6.2](#).

6-2.1 Chief Inspector

The chief inspector, as the security officer for the Postal Service, is responsible for the following:

- a. Issuing instructions and regulations on security requirements for personnel security.
- b. Establishing policies and procedures for overall Postal Service personnel security policies, including determining criteria for obtaining basic, nonsensitive, and sensitive clearances.
- c. Defining the criteria for the identification of sensitive positions.
- d. Determining whether a position is sensitive.
- e. Conducting background investigations of all personnel (see ASM 272).
- f. Granting all personnel clearances.

6-2.2 Manager, Corporate Information Security Office

The manager, Corporate Information Security Office (CISO), is responsible for the following:

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

- b. Assessing and ensuring compliance with personnel security policies related to information security through inspections, reviews, and evaluations.

6-2.3 **Contracting Officers**

Contracting officers are responsible for the following:

- a. Ensuring that all contracts requiring access to Postal Service information resources identify sensitive positions, specify the clearance levels required for the work, and address appropriate security requirements.
- b. Ensuring that the security provisions of the contract and business agreements are met.
- c. Confirming the employment status and clearance of all contractors requesting access to information resources.
- d. Ensuring all account references, building access, and other privileges are removed for contractor personnel when they are transferred or their employment terminated.

6-2.4 **All Managers**

Managers at all levels are responsible for the following:

- a. Ensuring that all personnel in their organization adhere to information security personnel policies and procedures.
- b. Identifying all sensitive information positions in their organizations related to information security and ensuring that personnel occupying sensitive positions hold the appropriate level of clearance.
- c. Funding background investigations and clearances.
- d. Notifying appropriate system and database administrators when access to information resources by personnel under your supervision is no longer needed due to changing job requirements.
- e. Reviewing all access privileges to information resources by personnel under your supervision semiannually and removing via eAccess those access privileges that are no longer needed.
- f. Documenting the security responsibilities of all personnel within their purview.
- g. Including employee security performance in performance evaluations.
- h. Supervising their contractor personnel in the absence of a contracting officer.
- i. Promulgating the security awareness program and ensuring personnel are trained in information security commensurate with their position and responsibilities.
- j. Processing departing (i.e., transferring to another organization or separating from the Postal Service) personnel appropriately and notifying the appropriate system and database administrators when personnel no longer require access to information resources.

- k. Initiating written requests for monitoring an individual's noncompliance with the acceptable use policies. For monitoring electronic messaging, follow the Management Instruction AS-870-2005-2: *Electronic Messaging (e-mail)* for the request and approval procedures on monitoring.

6-2.5 **All Personnel**

All personnel are responsible for the following:

- a. Performing the security functions and duties associated with their jobs.
- b. Complying with Postal Service information security policies and procedures.

6-2.6 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 6.2

Personnel Security Responsibilities

Activity	Chief Inspector	CISO	Contracting Officers	All Managers	All Personnel	OIG
Perform security responsibilities.					X	A
Include security in job descriptions & conduct performance appraisals.				X/F		A
Identify sensitive positions.	X		X	X		A
Conduct background investigations and clearances.	X			F		A
Conduct information security awareness training.		X/F		X/F		A
Process departing personnel.			X	X		A

X = Responsible for accomplishment

F = Responsible for funding

A = Independent audits, evaluations, and reviews

(See Appendix A for a consolidated list of roles and responsibilities.)

6-3 Employee Accountability

6-3.1 **Separation of Duties and Responsibilities**

6-3.1.1 **Required for Sensitive or Critical Information Resources**

Personnel with access to sensitive or critical information resources must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud, or collusion.

6-3.1.2 **Recommended for Business-Controlled Information Resources**

It may be recommended that certain personnel with access to business-controlled information resources not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud, or collusion. When it is not possible for duties to be assigned to separate individuals, the role performed must be clearly defined, associated activities logged, security-related functions audited, and compensating controls identified and implemented.

6-3.2 **Job Descriptions**

It is the intent of the Postal Service to define and document the information security requirements for each position.

6-3.3 **Performance Appraisals**

It is the intent of the Postal Service to evaluate the execution of information security responsibilities and the compliance with information security policies and procedures in personnel performance appraisals.

6-3.4 **Condition of Continued Employment**

It is the intent of the Postal Service to include the execution of information security responsibilities and the compliance with information security policies and procedures as a condition of continued employment for all personnel.

6-3.5 **Sanctions**

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

6-4 **Sensitive Positions**

6-4.1 **Definition of Sensitive Positions**

Sensitive positions, as defined in *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.

6-4.2 Identification of Sensitive Positions

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

6-5 Background Investigations and Clearances

6-5.1 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 will be restricted to baseline information services (see Section 9-4.2.1).

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

It is recommended that appropriate background investigations and personnel clearances be obtained for personnel who access business-controlled information resources.

6-5.2 Access Privileges

6-5.2.1 Logon IDs

For personnel without clearances, access privileges of the logon ID will be restricted baseline information services (see Section 9-4.2.1). 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.

6-5.2.2 Sensitive Resources

All personnel whose duties require access to sensitive or business-controlled sensitivity Postal Service information resources (see Chapter 3, Information Designation and Control) must have an appropriate clearance as determined by the Inspection Service before they obtain access (see ASM 272).

6-5.2.3 Controlled Areas

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

6-5.3 **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.

6-6 **Information Security Awareness and Training**

6-6.1 **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.

6-6.2 **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.

6-6.3 **Information Resource Operational Security Training**

For sensitive and critical information resources, appropriate operational security training must be developed and conducted. For business-controlled information resources, it is recommended that appropriate operational security training be developed and conducted. The training should explain how to protect application information throughout the lifecycle.

6-6.4 **New Personnel Training**

All new personnel must receive information security training.

6-7 **Departing Personnel**

6-7.1 **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, 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 information, in any format, in the custody of the terminating individual are returned, destroyed, or transferred to the custody of another individual.

6-7.2 **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. Ensure the return of accountable items and correct disposition of "RESTRICTED INFORMATION" as described under routine separation (see 6-7.1).
- e. Notify the Inspection Service.

6-7.3 **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 in 6-7.1 for routine separation or 6-7.2 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, CISO, of any information identified as removed but not recovered.

7 Physical and Environmental Security

7-1 Policy

The Postal Service will protect 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. Security requirements will extend to portable information resources and equipment, such as laptop computers, palmtops, and other hand-held devices, both on and off Postal Service premises.

7-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for physical and environmental security are defined in the sections below and are depicted in [Exhibit 7.2](#).

7-2.1 Chief Inspector

The chief inspector is responsible for the following:

- a. Establishing policy and criteria for overall Postal Service physical and environmental security.
- b. Providing physical protection assistance and investigating information security incidents involving the physical loss, theft, or destruction of Postal Service information resources.
- c. Conducting periodic site security reviews, surveys, and investigations of Postal Service activities and sites to evaluate all aspects of physical and environmental security.
- d. Providing technical guidance on physical security needs, such as controlled areas, access lists, physical access control systems, and identification badges.
- e. Providing technical guidance on physical and environmental security that supports information resources, including the protection of workstations, portable devices, and sensitive, critical, and business-controlled media.

- f. Providing guidance on the use of the Postal Service Security Force.
- g. Investigating reported violations of security regulations.

7-2.2 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Providing overall consultation and advice on Postal Service physical, environmental, and administrative security controls.
- b. Assessing the adequacy of physical, environmental, and administrative security controls in a changing information infrastructure.
- c. Assessing and ensuring compliance with physical security policies related to information security through inspections, reviews, and evaluations.

7-2.3 **Installation Heads**

Installation heads are responsible for the following:

- a. Designating a security control officer (SCO) who will be responsible for both 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, including support for information security, such as the protection of workstations, portable devices, and sensitive, critical, and business-controlled media.
- 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 security equipment and building modifications.
- e. Maintaining an accurate inventory of Postal Service information resources at their facility and implementing appropriate hardware security and configuration management.
- f. Maintaining and upgrading as necessary all security investigative equipment.
- g. Ensuring completion of a site security review, providing assistance to the Inspection Service and ISSO, as required, and accepting site residual risk.
- h. Ensuring that the Postal Service security policy, guidelines, and procedures are followed in all activities related to information resources at their facility, including procurement, development, and operation.
- i. Taking appropriate action in response to employees who violate established security policy or procedures.
- j. Developing facility continuity of operations (COOP) plans.

7-2.4 **Security Control Officers**

Security control officers (SCO) 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 sensitive or critical information resources.
- c. Establishing and maintaining access control lists of people who have 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 workstations and portable devices and sensitive, critical, and business-controlled media.
- f. Responding to physical security incidents.
- g. Reporting physical security incidents to the Inspection Service.
- h. Consulting on the facility continuity of operations (COOP) plans.

7-2.5 **Contracting Officers**

Contracting officers are responsible for the following:

- a. Ensuring appropriate security requirements are addressed in contracts requiring access to Postal Service information resources and facilities.
- b. Ensuring that the security provisions of the contract are met.
- c. Ensuring that building access and other privileges are removed for contractor personnel when they are transferred or terminated.

7-2.6 **All Personnel**

All personnel are responsible for the following:

- a. Displaying proper identification while in any facility that provides access to Postal Service information resources.
- b. Always using their physical and technology electromechanical access control identification badge or device to gain entrance to a controlled area.
- c. Ensuring no one tailgates into a controlled area on their badge.
- d. Protecting information resources, including workstations, portable devices, information, and media.
- e. Being aware of their physical surroundings, including weaknesses in physical security and the presence of any authorized or unauthorized visitor.
- f. Promptly reporting suspicious or potentially dangerous activities or conditions (see Chapter 13, Incident Management).
- g. Taking immediate action to protect the information resources at risk upon discovering a security deficiency or violation.

7-2.7 Inspector General

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 7.2

Physical and Environmental Security Responsibilities

Activity	Chief Inspector	CISO	Installation Heads	Contracting Officers	SCOs	All Personnel	OIG
Establish controlled areas & access control lists.	C/R	C	X/F	K	X		A
Install physical access control devices & implement identification badges.	C/R	C	X/F	K	C		A
Protect network equipment, servers, & mainframes.	C/R	C	X/F	K	X		A
Protect workstations, portable devices, information, & media.	C/R	C	X/F	K	C/R	X	A
Implement environmental security & support continuity of operations planning.	C/R	C	X/F	K	C		A

X = Responsible for accomplishment

F = Responsible for funding

C = Consulting support as required

K = Include requirements in contracts

R = Reviewing as required

A = Independent audits, evaluations, and reviews

(See Appendix A for a consolidated list of roles and responsibilities.)

7-3 Facility Security

All 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. For additional information, see Handbook RE-5, *Building and Site Security Requirements*. Such physical and administrative security controls include:

- a. Physical access control.
- b. Physical protection of information resources.
- c. Environmental security.
- d. Continuity of operations (COOP) plan.

7-3.1 Physical Access Controls

7-3.1.1 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.

7-3.1.2 **Types of Information Resources Stored in Controlled Areas**

Sensitive and critical information resources must be located in a controlled area. It may be recommended that certain business-controlled information resources be located in a controlled area.

7-3.1.3 **Access to Controlled Areas**

Access to controlled areas is restricted to personnel whose duties require access to such facilities and who possess appropriate security clearances. Access to controlled areas must be authorized and tailgating is not allowed.

Access to controlled areas must be controlled by electromechanical means. Personnel authorized access to the controlled areas must always use their physical and technology electromechanical access control identification badge or device to gain entrance to the controlled area. It is their responsibility to ensure no one tailgates on their badge.

Personnel without an authorized physical and technology electromechanical access control identification badge or device must be escorted by authorized personnel while in the controlled area.

7-3.1.4 **Establishment of Access Control Lists**

Each controlled area must establish an access control list of people who are authorized access to specific control areas. 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.

7-3.1.5 **Training for Controlled Areas**

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

7-3.1.6 **Installation of Physical Access Control Devices**

Physical access control devices using biometrics, smart cards, tokens, CCTV, alarms, mantraps, or lockable cabinets will be installed to supplement traditional facility locks and keys to limit access.

7-3.1.7 **Implementation of Additional Physical Access Security**

7-3.1.7.1 **Required for Sensitive or Critical Information Resources**

Additional physical access security (e.g., locked cabinet or desk, biometric workstation lock), based on risk associated with the information resource, must be implemented for sensitive and critical information resources.

7-3.1.7.2 **Recommended for Business-Controlled Information Resources**

It is recommended that additional physical access security (e.g., locked cabinet or desk, biometric workstation lock), based on risk associated with the information resource, be implemented for business-controlled information resources.

7-3.1.8 **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.

Note: It is recommended that the organization manager or designee make an unannounced verification of badges at least annually to ensure authenticity and to correct any badge discrepancies.

7-3.2 **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 and business-controlled sensitive information on information resources must be encrypted in transit. Sensitive and business-controlled sensitive information stored on removable devices or

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

7-3.2.1 **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.

7-3.2.2 **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.

7-3.2.3 **Non-Postal Service Portable Devices**

In order to protect Postal Service information from disclosure or compromise, non-Postal Service portable devices (e.g., laptops, notebooks, personal digital assistants [PDAs], handheld computers, cameras, watches with cameras, or storage media including universal serial bus [USB] port devices or thumb drives) should not be used on Postal Service facilities without written 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 will determine if such devices must be surrendered for the duration of the visit. Under no circumstances will such devices connect to the Postal Service Intranet (Blue) or store Postal Service information.

7-3.2.4 **Sensitive, Critical, and Business-Controlled Media**

Sensitive, critical, and business-controlled 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 and business-controlled sensitivity information. Personnel who have custody of sensitive, critical, or business-controlled media are responsible for their safekeeping (see Chapter 3).

7-3.3 **Environmental Security**

Environmental security controls must be implemented at the facility, room, and information resource level to protect critical and business-controlled criticality information resources as described below:

- a. Safeguards must provide protection against lightning, wind, and building collapse.

- b. Redundant power feeds, redundant communications paths, and additional temperature and humidity controls are recommended for facilities hosting critical and business-controlled criticality information resources.
- c. Water and sewer utilities and the potential for flood, earthquakes, or other natural disasters must be evaluated for facilities hosting critical information resources. It is recommended that water and sewer utilities and the potential for flood, earthquakes, or other natural disasters be evaluated for facilities hosting business-controlled criticality information resources.
- d. Surge protection must be implemented for all information resources.
- e. Additional fire safeguards and additional power (electricity) controls must be implemented for critical information resources and are recommended for business-controlled criticality information resources.

7-3.4 **Facility Business Continuity Management Planning**

Physical security requirements must be included in facility business continuity management (BCM) planning to ensure the appropriate protection of information resources following a catastrophic event (see Chapter 12).

7-3.5 **Facility Contracts**

Information, environmental, and physical security requirements must be included in contracts involving services performed for the Postal Service.

8 System, Applications, and Product Development

8-1 Policy

Information resources must be developed under a formal system development methodology. Information security must be an integral part of the system development life cycle whether development is done in house, acquired, or outsourced. The Postal Service information security assurance (ISA) process defines a formal review process that ensures adequate security is incorporated during each phase of the system life cycle.

8-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for system, application, and product development are defined in the sections below and are depicted in [Exhibit 8.2](#).

8-2.1 Chief Inspector

The chief inspector is responsible for 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.

8-2.2 Vice President, Chief Technology Officer

The vice president, Chief Technology Officer (VP/CTO), is responsible for the following:

- a. Ensuring the technical security controls required for business functionality are implemented.
- b. Accepting residual risk to applications jointly with the vice president of the appropriate functional business area. The VP/CTO has delegated this responsibility to the applicable manager, business systems portfolio (portfolio manager).

- c. Approving an application for deployment jointly with the vice president of the functional business area. The VP/CTO has delegated this responsibility to the applicable portfolio manager.

8-2.3 **Vice Presidents, Functional Business Areas**

Vice presidents of functional business areas are responsible for the following:

- a. Approving and funding the development of information resources.
- b. Ensuring resources are available for completing security tasks.
- c. Ensuring the security of all information resources within their organization.
- d. Accepting residual risk to applications jointly with the VP/CTO. The vice presidents of functional business areas have delegated this responsibility to the applicable executive sponsor.
- e. Approving an application for deployment jointly with the VP/CTO. The vice presidents of functional business areas have delegated this responsibility to the applicable executive sponsor.
- f. Ensuring that contractual agreements require all contractors, vendors, and business partners to adhere to Postal Service security policies and provide current information security plans.

8-2.4 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Providing guidance and oversight on application security.
- b. Providing overall consultation and advice on the Postal Service ISA process.
- c. Assessing and ensuring compliance with information security policies related to system, application, and product development through inspections, reviews, and evaluations.
- d. Reviewing the ISA documentation package and accrediting the application.

8-2.5 **Executive Sponsors**

Executive sponsors, as representatives of the vice president of the functional business area, are the business managers with oversight (funding, development, production, and maintenance) of the information resource and are ultimately responsible for ensuring the completion of all security-related tasks throughout the life cycle of an information resource. In particular, executive sponsors are responsible for the following for each information resource within their purview:

- a. Funding and implementing information security and ISA procedures throughout the life cycle.
- b. Conducting a business impact assessment (BIA) to determine sensitivity and criticality.

- c. Conducting a risk assessment to analyze threats, vulnerabilities, and risks.
- d. Appointing, in writing, an information systems security representative (ISSR).
- e. Ensuring that all information security requirements are implemented and maintained.
- f. Ensuring that all information security requirements are included in contracts and strategic alliances.
- g. Working jointly with the portfolio manager to review the ISA documentation package and make one of the following decisions: accept the residual risk to an application and approve the application for production or return the application to the applicable lifecycle phase for rework.

8-2.6 **Portfolio Managers**

Portfolio managers are responsible for the following:

- a. Functioning as liaisons between executive sponsors and the information technology providers.
- b. Supporting the executive sponsor in the development of an application and the documentation required by the ISA process, including the business impact assessment, risk assessment, security plan, security test and evaluation plan, and application disaster recovery plan.
- c. Ensuring the application is entered into the Enterprise Information Repository (EIR) and updated as required.
- d. Appointing, if desired, an information systems security representative (ISSR) to perform security-related activities.
- e. If a documented vulnerability will not be mitigated, preparing and signing an acceptance of responsibility letter as part of the ISA process.
- f. Reviewing the ISA documentation package and completing a risk mitigation plan for risks identified as High or Medium.
- g. Working jointly with the executive sponsor to review the ISA documentation package and make one of following decisions: accept the residual risk to an application and approve the application for production, or return the application to the applicable lifecycle phase for rework.
- h. Ensuring that the application is registered in eAccess.
- i. Accepting personal accountability for adverse consequences if application was placed in production before the Application ISA process was completed.

8-2.7 **Project Managers**

Project managers for the information resource development, acquisition, or integration project are responsible for the following:

- a. Managing day-to-day development and implementation efforts for new information resources.
- b. Incorporating the appropriate security controls in all information resources.
- c. Updating the EIR on behalf of the portfolio manager.

8-2.8 **Accreditor**

The manager, Corporate Information Security Office, functions as the accreditor and is responsible for the following:

- a. Reviewing the risk mitigation plan and supporting ISA 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 application 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 ISA documentation package to the portfolio manager and executive sponsor.

8-2.9 **Certifier**

The manager, Information Security Assurance, who is appointed by the CISO, functions as the certifier and is responsible for the following:

- a. Managing and providing guidance to the information systems security officers (ISSOs).
- b. Reviewing the ISA evaluation report and the supporting ISA documentation package.
- c. Escalating security concerns or preparing and signing a certification letter.
- d. Forwarding the certification letter and ISA documentation package to the portfolio manager.
- e. Maintaining an inventory of all information resources that have completed the ISA process.

8-2.10 **Information Systems Security Officers**

Information systems security officers (ISSOs) are assigned to portfolios by the manager, CISO. ISSOs are responsible for the following:

- a. Providing information security and ISA guidance.
- b. Chairing the ISA team and leading the ISA process.

- c. Providing advice and consulting support to executive sponsors regarding the security requirements and controls necessary to protect information resources based on their sensitivity and criticality.
- d. Providing guidance on the applicability of threats and vulnerabilities, appropriate choice of countermeasures, and the ISA process.
- e. Reviewing the ISA package.
- f. Preparing the evaluation report and forwarding the evaluation report and ISA documentation package to the certifier.

8-2.11 **Information Systems Security Representatives**

Information systems security representatives (ISSRs), who are appointed in writing by the executive sponsors or portfolio managers, 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 ISA process as assigned by the executive sponsor or portfolio manager.
- f. Organizing the ISA documentation package and forwarding the package to the ISSO.

8-2.12 **Contracting Officers and Contracting Officer Representatives**

Contracting officers and contracting officer representatives are responsible for the following:

- a. Ensuring information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, standards, and procedures.
- b. Ensuring that the security provisions of the contract and business agreements are met.
- c. Ensuring contracts and agreements are in place that allow monitoring and auditing of any information resource project.

8-2.13 **General Counsel**

General counsel is responsible for the following:

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

- b. Ensuring contracts and agreements are in place which allow monitoring and auditing of any information resource project.

8-2.14 Business Partners

Business partners developing information resources for the Postal Service must abide by Postal Service information security policies regardless of where the systems are located or who operates them. This requirement includes business partners involved in strategic alliances with the Postal Service.

8-2.15 Chief Privacy Officer

The chief privacy officer (CPO) is responsible for consulting on and reviewing the BIA during development and following completion.

8-2.16 Inspector General

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 8.2

System, Application, and Product Development Responsibilities

Activity	Executive Sponsors	Portfolio Managers	Project Managers	ISSOs	ISSRs	Certifier ¹	Accreditor ²
Initiate ISA & conduct BIA.	X/F	C	P	P	P		
Conduct risk assessment.	X/F	C	P	P	P		
Identify security controls.	X/F	C	P	C	P		
Develop security plan & develop/acquire security controls.	X/F	C	P	C	P		
Develop SOPs, service level & trading partner agreements.	X/F	C	P	C	P		
Develop security test plan.	X/F	C	P	C	P		
Conduct security testing & document results.	X/F	C	X	C	P		
Conduct independent reviews as required.	X/F	C	P	C	P		
Develop ISA package.	X/F	C	P	P	X		
Review ISA package & write evaluation report.				X			

Activity	Executive Sponsors	Portfolio Managers	Project Managers	ISSOs	ISSRs	Certifier ¹	Accreditor ²
Certify application.	F					X	
Prepare risk mitigation plan and accept responsibility for documented vulnerabilities.	F	X		C			
Accredit application.	F						X
Accept risk & approve for deployment.	X	X	C	C		C	C
Develop and test ADRP & FR Plan	X/F	C	P	C	P		
Follow security-related plans, periodically review, test, and audit.	X/F	C	P	C	P		
Reassess risks & upgrade controls, update security-related documents.	X/F	C	P	C	P		
Re-initiate ISA.	X/F	C	P	X	P		X
Retire application.	X/F	C	P	C	P		

¹ Manager, ISA Process.

² Manager, Corporate Information Security Office (CISO)

X = Responsible for accomplishment

F = Responsible for funding

P = Participant

C = Consulting support as required

Other organizations and managers responsible for system, application, and product development include: chief inspector; inspector general; chief privacy officer; contracting officers and general counsel; and business partners (see Appendix A, *Consolidated Roles and Responsibilities*, for details).

8-3 General Development Concepts

The following requirements apply to all sensitive, critical, and business-controlled applications:

- a. Developers must not have access to production application systems software.
- b. Developers' access to production information must be authorized in writing by executive sponsors.
- c. Access to production information, if approved, must be temporary.
- d. Production data must not be copied.

- e. Audit logging must be turned on.
- f. Keystroke logging must be implemented.

8-3.1 Life Cycle Approach

Sensitive, critical, and business-controlled information resource development must utilize a formal system development methodology (SDM). Security must be addressed throughout the information resource life cycle process, from conception through design, development, deployment, operation, and retirement from service. All development, acquisition, or integration projects for information resources, whether performed in house or by a business partner, must incorporate the following general life cycle concepts:

- a. A comprehensive risk management approach.
- b. A quality assurance program that includes information security testing.
- c. Rigorous configuration management and change control processes.
- d. Separation of duties.
- e. Restrictions associated with testing.
- f. Information security in all phases of the information resource life cycle.

8-3.2 Risk Management

A secure computing environment must be implemented that is based on managing risks to an acceptable level. A risk-based approach to information security promotes using 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 Chapter 4, Risk Management).

8-3.3 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.

8-3.4 Change Control, Version Control, and Configuration Management

All information resources, whether developed in house, outsourced, or acquired, must be developed under rigorous change control, version control, and configuration management procedures to reduce the risk introduced by undocumented and untested changes (see the Postal Service change and configuration management process at <http://blue.usps.gov/changemgmt>). Postal Service information resources must not be developed or deployed unless a change control process is in place.

8-3.5 **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.

8-3.6 **Development and Test Environment 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.

8-3.6.1 **Separation of Development/Test and Production Environments**

Hardware and software must be developed and tested in a test environment — not in a production environment.

8-3.6.2 **Testing with Nonsensitive Production Data**

Prior approval in writing is required from the executive sponsor and VP/CTO, 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.

8-3.6.3 **Testing with Sensitive and Business-Controlled Sensitivity Production Data**

Prior approval in writing is required from the CPO, executive sponsor, and VP/CTO if sensitive data, business-controlled sensitivity data, Privacy Act data, personally identifiable information (PII), or any information identified as “RESTRICTED INFORMATION” is to be used in a test environment, regardless of where the testing is conducted. Such approved data files must be identified as “copies” to prevent them from being re-entered into the production environment.

8-3.6.4 **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 Security Activities and the Development Life Cycle

System development methodologies in use at the Postal Service and by its vendors may identify life cycle phases differently. Each phase of the life cycle will have corresponding security activities that must be performed to maintain a secure environment and comply with Postal Service policies and legal requirements. For purposes of discussion, the required security activities are presented in the Information Security Assurance (ISA) process.

8-5 Information Security Assurance Process

The ISA process is a formal security analysis and management approval process to assess residual risk before the resource is put into production. The ISA process is required for each information resource (i.e., application or infrastructure component).

8-5.1 **What the ISA Process Covers**

The ISA process consists of five interrelated phases that are conducted concurrently with the development and deployment of new information resources and every 5 years during the life cycle of the information resource. The objectives of the ISA 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 critical, sensitive, and business-controlled resources, the ISA culminates with the certification, accreditation, and approval to deploy the information resource. All wireless information resources, regardless of sensitivity or criticality, must complete the full ISA process.

8-5.2 **When ISA Is Required**

The ISA is required for the following:

- a. All information resources, regardless of where they are located 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.

8-5.3 **Value of the ISA Process to the Postal Service**

ISA 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.

8-5.4 **Access to Information Resources and Related Documentation**

During the ISA process, the manager, Corporate Information Security Office, or designated agent will have unrestricted access to the information resources and related documentation.

8-5.5 **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 (see 8-6.3.5).
- b. Independent security code review (see 8-6.3.6).
- c. Independent penetration testing and vulnerability scans (see 8-6.3.8).
- d. Independent security test validation (see 8-6.3.9).

8-6 Application Information Security Assurance Phases

[Exhibit 8.6](#) depicts the five phases and the major documents (deliverables) for each phase. The purpose and information security activities associated with the ISA phases are as follows:

8-6.1 **Phase 1 — Definition**

Phase 1 determines what will be required during the ISA and the magnitude of the effort needed to complete the ISA process. Phase 1 usually begins with a meeting of the executive sponsor and ISSO to review the ISA process and complete the business impact assessment (BIA) process. The information security activities of Phase 1 are as follows:

8-6.1.1 **Initiate Application Information Security Assurance Process**

The ISA process is initiated for all applications regardless of where they are located or whether they are controlled directly by the Postal Service or through a contractor or business partner.

8-6.1.2 **Assign Information Systems Security Representative**

The executive sponsor or portfolio manager may assign in writing an information systems security representative (ISSR) to perform security-related activities.

8-6.1.3 **Conduct Business Impact Assessment**

A BIA is completed (see Chapter 3) to determine the level of sensitivity and criticality, and the information security requirements for the application.

8-6.1.4 **Define Security Requirements**

Security requirements are defined for all applications so the applications can be secured commensurate with the risk. Security requirements include the baseline security requirements for all applications and additional mandatory security requirements based upon how sensitive or critical the applications are (as defined by the ISA process); federal legislation, regulation, and directives; industry requirements; operating environment; and risks associated with the information resource. (See Handbook AS-805, *Information Security*, Chapter 3, Information Designation and Control, 3-4.4, Mandatory Security Requirements, for examples.) As an example, payment card applications must comply with the payment card industry (PCI) requirements. In addition, the ISSO may recommend additional discretionary security requirements based on generally accepted industry practices that the executive sponsor may agree to implement.

8-6.1.5 **Document High-Level Architecture**

A high-level architectural diagram (e.g., hardware, communications, security devices, and interconnected resources) is developed for all applications. The architectural diagram is submitted to the manager, SIS, for review and determination of the impact on the infrastructure and the need for additional security controls for the application (e.g., enclave).

8-6.1.6 **Document Information Resources in the Enterprise Information Repository**

All applications are documented in the Enterprise Information Repository (EIR).

8-6.2 **Phase 2 — Design and Integration**

Based on the baseline, mandatory, and selected approved discretionary security requirements from the BIA, the security controls and processes for the application are defined and implemented. The information security activities of Phase 2 are as follows:

8-6.2.1 **Conduct Risk Assessment**

A risk assessment is conducted for sensitive, critical, and business-controlled applications to identify security concerns (threats, vulnerabilities, control weaknesses), risk ranking, additional countermeasures, and residual risk (see Chapter 4).

8-6.2.2 Identify Security Controls

Security controls are identified for potential threats and vulnerabilities as a result of the risk assessment process (see Chapter 4). Security controls, when appropriately implemented, provide protection of applications from threats and vulnerabilities.

8-6.2.3 Perform Controls Analysis

An analysis of identified controls (safeguards) is conducted to determine their potential effectiveness to remove, transfer, or otherwise mitigate risk to applications. The controls analysis identifies any residual risk to the application.

8-6.2.4 Perform Cost Benefit Analysis

A cost benefit analysis is performed and documented to facilitate the implementation of cost-effective protection for applications and continuity of business operations.

8-6.2.5 Document Security Specifications

Security specifications are documented to satisfy the security requirements defined by the BIA. Safeguards are selected or designed, purchased or built, and configured to address the security specifications and bring residual risk to an acceptable level by reducing the likelihood of occurrence that a vulnerability will be exploited and by reducing the amount of harm that could occur if a vulnerability is exploited.

8-6.2.6 Develop Security Plan

A security plan is developed for sensitive, critical, and business-controlled applications. A security plan is a blueprint for designing, building, and maintaining an application 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.

8-6.2.7 Develop or Acquire Security Controls

Appropriate security controls are developed in house, acquired, or outsourced, depending on the cost benefit analysis.

8-6.2.8 Harden Information Resources

Information resources hosting applications are 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.

8-6.2.9 Develop Application Disaster Recovery Plan

An application disaster recovery plan (ADRP) is developed for critical applications and for business-controlled criticality applications (see Chapter 12, Business Continuity Management).

8-6.2.10 Develop Facility Recovery Plan

A facility recovery plan is developed for facilities designated by the VP/CTO as major information technology sites (see Chapter 12, Business Continuity Management).

8-6.2.11 Develop Standard Operating Procedures

Standard operating procedures (SOPs) for emergency procedures, separation of duties, computer operations, manual processes, etc., must be developed for sensitive, critical, and business-controlled information resources.

8-6.2.12 Incorporate Security Requirements in SLAs and Trading Partner Agreements

Service level agreements (SLAs) are developed for all applications. Trading partner agreements are developed for all externally managed and/or developed applications. Information security requirements are addressed in all SLAs and trading partner agreements.

8-6.2.13 Develop Operational Security Training

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

8-6.2.14 Register Application in eAccess

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

8-6.3 Phase 3 — Testing

The security controls and processes defined in the security plan and implemented in Phase 2 are tested. The information security activities of Phase 3 are as follows:

8-6.3.1 Develop Security Test Plan

A security test plan is developed for sensitive, critical, and business-controlled applications. The security test plan evaluates the technical and nontechnical security controls and other safeguards to establish the extent to which the application meets the security requirements for its mission and operational environment. The security test plan also addresses hardware, operating system, networking and telecommunications,

physical security, personnel security, and computer operations and manual processes.

8-6.3.2 **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 application and its security safeguards.

8-6.3.3 **Conduct Security Code Review**

To protect the infrastructure, a documented security code review is required for any externally facing, publicly available, or demilitarized zone (DMZ)-hosted application containing custom programming or scripting, regardless of the designation of sensitivity or criticality.

A code review is required for sensitive and critical applications that contain active content code or CGI scripts. A code review is recommended for business-controlled applications that contain active content code or CGI scripts.

The security code review will be based on the Postal Service *Security Code Review Standards* or an acceptable equivalent. This security code review will not be required if an independent security code review is conducted (see 8-6.3.6.2).

8-6.3.4 **Conduct Vulnerability Scan**

A vulnerability scan is recommended for all information resources and applications, and is required for some information resources and applications (see Handbook AS-805-A, *Application Information Security Assurance [ISA] Process*).

8-6.3.5 **Conduct Independent Risk Assessment**

See Chapter 4, Risk Management, for a description of and criteria for conducting an independent risk assessment.

8-6.3.6 **Conduct Independent Security Code Review**

8-6.3.6.1 **Independent Security Code Review Description**

Custom programs or commercial-off-the-shelf (COTS) applications that contain custom programming or scripts 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, efficiency, and specific security issues.

8-6.3.6.2 **Criteria for Conducting an Independent Security Code Review**

An independent security code review is recommended by the ISSO during the BIA process for the following resources:

- a. Critical or sensitive applications developed externally.

- b. COTS products or applications containing custom programming or scripts that support a sensitive or critical application.
- c. Applications (including COTS applications containing custom programming), regardless of the designation of sensitivity or criticality, that transmit information between a Postal Service network and an external network, or between a Postal Service demilitarized zone (DMZ) and an external network.
- d. External facing Web-based applications, regardless of the designation of sensitivity or criticality, containing custom programming (HTML, XML, Java, Javascript, CGI, ActiveX, etc.).

Note: An independent code review may be required at any time by the VP/CTO; manager, CISO; or vice president of the functional business area.

Note: The application developer is responsible for ensuring that the application has been designed and constructed in a secure manner; therefore, the developer is responsible for the funding of subsequent independent code reviews if they are required.

8-6.3.7 **Conduct Security Testing and Document Results**

Security testing is performed for sensitive, critical, and business-controlled applications. The executive sponsor must ensure that security testing is conducted using the approved security test plan. The platform and application technical mechanisms and the surrounding administrative controls are evaluated to establish the extent to which the application meets the security requirements.

8-6.3.8 **Conduct Independent Penetration Testing and Vulnerability Scans**

8-6.3.8.1 **Independent Penetration Testing and Vulnerability Scans Description**

The independent penetration testing and vulnerability scans evaluate the effectiveness of the implemented information resource configuration. These tests scan information resources for vulnerabilities and compliance with Postal Service information security policies and standards.

8-6.3.8.2 **Criteria for Conducting Independent Penetration Testing and Vulnerability Scans**

Independent penetration testing and vulnerability scans are recommended by the ISSO during the BIA process for information resources hosting the following types of applications:

- a. Sensitive, critical, and business-controlled applications.
- b. Publicly accessible (externally facing) applications.
- c. Applications that have access to or communicate through an untrusted network.

- d. Applications developed, hosted, or managed primarily by non-Postal Service personnel.

Note: Independent penetration testing and vulnerability scans may be required at any time by the VP/CTO; manager, CISO; or vice president of the functional business area.

8-6.3.9 **Conduct Independent Validation of Security Testing**

8-6.3.9.1 **Independent Validation of Security Testing Description**

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 application, its hosting information resources, its environment, and the associated threats and vulnerabilities. The independent security test validation is usually carried out at the development or test site.

8-6.3.9.2 **Criteria for Conducting Independent Validation of Security Testing**

An independent security test validation is recommended by the ISSO during the BIA process for the following applications:

- a. Publicly accessible (externally facing) applications.
- b. Applications that have access to, or communicate through, an untrusted network.
- c. Applications developed, hosted, or managed primarily by non-Postal Service personnel.

Note: An independent security test validation may be required at any time by the VP/CTO; manager, CISO; or vice president of the functional business area.

8-6.3.10 **Address Outstanding Issues**

Outstanding issues are addressed and the residual risk for applications is identified and documented. The residual risk is that portion of risk that remains after the security safeguards and countermeasures have been applied.

8-6.4 **Phase 4 — Evaluation**

Phase 4 consists of activities described below that culminate in the certification, risk mitigation plan, accreditation, acceptance of residual risk, and approval to deploy an application:

- a. **ISA Evaluation Report**
The ISSO evaluates the ISA documentation, prepares an ISA evaluation report that details the findings, and escalates security concerns or forwards the ISA evaluation report and the ISA documentation package to the certifier.
- b. **Certification**

The certifier reviews the ISA evaluation report and ISA documentation package, escalates security concerns or certifies the application by preparing and signing a certification letter, and forwards the certification letter and ISA documentation package to the portfolio manager.

c. Risk Mitigation

The portfolio manager analyzes the ISA and business documentation, escalates security concerns or prepares a risk mitigation plan which addresses High and Medium risks, and forwards the risk mitigation plan and ISA documentation package to the accreditor.

d. Accreditation

The accreditor analyzes ISA and business documentation, escalates security concerns or prepares an accreditation letter, and forwards the accreditation letter and ISA documentation package to the executive sponsor and portfolio manager.

e. Acceptance of Residual Risk and Approval of Application for Deployment

The executive sponsor and portfolio manager jointly review the ISA and business documentation and return the application to the applicable ISA phase for rework or approve the application for deployment in the production environment by preparing and signing an acceptance letter.

The information security activities of Phase 4 are as follows:

8-6.4.1 **Develop ISA Documentation Package**

Sensitive, critical, and business-controlled applications require an ISA 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 ADRP); and the security test and evaluation results.

8-6.4.2 **Review ISA Documentation Package and Write Evaluation Report**

The ISSO reviews the ISA documentation package and writes an ISA evaluation report highlighting the findings and recommendations. The ISSO escalates security concerns or forwards the ISA evaluation report and supporting documentation to the certifier for review.

8-6.4.3 **Escalate Security Concerns or Certify Application**

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

8-6.4.4 **Escalate Security Concerns or Prepare Risk Mitigation Plan**

The portfolio manager reviews the certification letter and the supporting ISA 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 accreditor then forwards the risk mitigation plan and ISA documentation package to the accreditor.

8-6.4.5 **Escalate Security Concerns or Accreditation Application**

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

8-6.4.6 **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 ISA documentation package. They will issue a joint decision on whether to accept the residual risk and approve the application for deployment with what restrictions, if any.

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

8-6.4.7 **Deploy Application**

When the application is deployed, the security controls for the application are implemented as documented in the security plan and the acceptance letter.

8-6.5 **Phase 5 — Production**

Phase 5 is the operation and maintenance period of the application 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 application. The information security activities for Phase 5 are as follows:

8-6.5.1 **Application Maintenance**

Applications must be maintained in a timely manner. The tools, techniques, and mechanisms used to maintain application systems must be properly controlled.

8-6.5.2 **Follow Security-Related Plans and Continually Monitor Operations**

The security-related plans are executed as required during deployment, operation, and maintenance. The application is continually monitored for compliance with the security-related plans.

8-6.5.3 **Periodically Review, Test, and Audit**

Applications are periodically reviewed and audited for compliance with Postal Service policies. Plans related to facility recovery or business continuity are

tested to ensure that these plans meet business and security objectives (see Chapter 12, Business Continuance Management).

8-6.5.4 **Re-assess Risks and Upgrade Security Controls**

Risks are re-assessed every 5 years, at any time major changes are made to the application, if a serious security breach occurs, or if audit findings regarding security are issued. Security controls are upgraded as necessary to protect the application and assure business continuity.

8-6.5.5 **Update Security-Related Plans**

Security-related plans are updated in response to changing environment, changing technology, and other re-assessed risks.

8-6.5.6 **Re-initiate ISA**

Re-initiating the ISA is required a minimum of every 5 years following the initial ISA of the application. Re-initiating the ISA may result in re-certification, re-accreditation, re-acceptance of risk, and re-approval for deployment.

Re-initiating the ISA could also be required for the following reasons:

- a. Significant changes to the operating environment or the business requirements of the application. Significant changes may include, but are not limited to:
 - (1) Change in the functions of the application or data that alters the criticality or sensitivity designation of the application.
 - (2) Change from one major application to another, such as BroadVision to WebObjects.
 - (3) Change from one database application to another, such as Oracle to MS-SQL.
 - (4) Change in the hosting location, such as from a Postal Service facility to an out-sourced, 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 application.
- b. A significant information security incident that violates an explicit or implied security policy, compromising the integrity, availability, or confidentiality of an application (e.g., a critical disruption or monetary loss, the unauthorized modification of sensitivity or criticality information, or the release of sensitive or business-controlled sensitivity information).
- c. A significant finding of an audit or other external assessment.
- d. A request by the VP/CTO; the manager, CISO; the vice president of the functional business area; or the executive sponsor.

8-6.5.7 **Retain ISA Documentation**

Upon completion of the ISA process, the executive sponsor is responsible for retaining the ISA documentation package.

8-6.5.8 Retire Information Resource**8-6.5.8.1 Disposal of Data**

All Postal Service sensitive and business-controlled sensitivity 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 Handbook AS-353).

8-6.5.8.2 Sanitize Equipment and Media

All Postal Service sensitive or business-controlled sensitivity information is completely erased or destroyed prior to disposal of the hardware or electronic media on which it resides (see 3-6).

8-7 Business Partnerships and Alliances

8-7.1 Policy Compliance

All contractors, vendors, and business partners who are developing information resources for the Postal Service must abide by Postal Service information security policies regardless of where the systems are located or who operates them.

8-7.2 ISA Requirement

The ISA process applies to all Postal Service information resources sponsored by, endorsed by, or developed for the benefit of the Postal Service, whether located at a Postal Service or non-Postal Service facility.

8-7.3 Contractual Terms and Conditions

Contract language and partnering agreements must reflect the information security requirements of the Postal Service as defined in this document and as generated in the ISA process. The executive sponsor is responsible for ensuring that security plan 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.

9 Information Security Services

9-1 Policy

Information security services will be implemented to ensure a viable secure computing infrastructure and to protect information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. Information security services in the Postal Service will include those controls needed to manage access, ensure accountability, protect confidentiality, maintain data integrity, administer security controls, and capture audit information for information resources.

9-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for information security services are defined in the sections below and are depicted in [Exhibit 9.2](#).

9-2.1 **Chief Information Officer/Vice President, Information Technology**

The chief information officer/vice president, Information Technology (CIO/VP IT), is responsible for the following:

- a. Identifying and authorizing baseline information resource services for personnel.
- b. Assigning data to an organizational entity for stewardship.

9-2.2 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Serving as the central point of contact for all information security issues and providing overall consultation and advice on information security policies, processes, requirements, controls, services, and issues.
- b. Developing information security policies, processes, and procedures.
- c. Assessing the adequacy of information security processes in a changing information infrastructure and updating those processes as necessary.

- d. Providing guidance and oversight for security architecture, technologies, and controls.
- e. Providing guidance on the implementation of information security services.
- f. Providing guidance on biometrics, smart cards, tokens, and other access control technologies.
- g. Approving establishment of shared accounts.
- h. Assessing and ensuring compliance with information security services policies through inspections, reviews, and evaluations.

9-2.3 **Managers, Computing Operations/Infrastructures**

The managers, computing operations/infrastructures (e.g., managers, Host Computing Services, Customer Care Operations, Engineering), are responsible for the following in the mainframe, distributed, and engineering environments:

- a. Implementing and maintaining security throughout the mainframe, distributed, and engineering infrastructures.
- b. Ensuring remote access is appropriately managed.
- c. Implementing appropriate security administration and managing accounts appropriately.
- d. Maintaining the integrity of data and information resources.
- e. Implementing information security policies, procedures, and hardening standards.
- f. Ensuring the appropriate level of information resource availability.
- g. Ensuring infrastructure availability through planning for capacity, scalability, and redundancy.

9-2.4 **Manager, Secure Infrastructure Services**

The manager, Secure Infrastructure Services (SIS), is responsible for the following:

- a. Implementing and maintaining a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.
- b. Implementing secure identification and authentication mechanisms, including strong authentication, digital certificates, digital signatures, biometrics, smart cards, tokens, and the associated infrastructure.
- c. Ensuring that only Postal Service-approved encryption products are used with information resources.
- d. Implementing security controls and processes that will safeguard the availability and integrity of the Managed Network Services (MNS).
- e. Implementing appropriate security administration and managing accounts appropriately.
- f. Setting standards for session management.

- g. Maintaining the integrity of data and information resources.
- h. Ensuring the appropriate level of information resource availability.
- i. Implementing and managing the computer incident response team (CIRT).
- j. Ensuring infrastructure availability through planning for capacity, scalability, and redundancy.
- k. Implementing appropriate remote access controls.

9-2.5 **Executive Sponsors**

Executive sponsors are responsible for the following:

- a. Providing resources to ensure security requirements are properly addressed.
- b. Ensuring that information resources within their purview are capable of enforcing appropriate levels of security services.
- c. Authorizing access to the information resources under their control.
- d. Reviewing access authorizations on a semiannual basis for personnel under their purview who access information resources.
- e. Implementing encryption to protect restricted information as required.
- f. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.
- g. Developing information resources with protection mechanisms that assure data integrity.
- h. Ensuring the availability of information resources under their purview.
- i. Ensuring information resource availability through planning for capacity, scalability, and redundancy.

9-2.6 **All Managers**

Managers at all levels are responsible for the following:

- a. Providing resources, including personnel, financial, and physical assets, to meet information security requirements.
- b. Approving requests by personnel under their supervision for access to information resources beyond baseline services.
- c. Reviewing access authorizations for personnel under their supervision on a semiannual basis.
- d. Notifying the appropriate system and database administrators when personnel no longer require access to information resources.
- e. Ensuring the availability of information resources under their control.
- f. Complying with appropriate information security policies and procedures.

9-2.7 **System Administrators**

System administrators are responsible for the following for information resources under their control:

- a. Implementing information security policies and procedures and monitoring the implementation for proper functioning of security mechanisms.
- b. Implementing appropriate platform security based on the platform-specific hardening guidelines.
- c. Complying with standard configuration settings, services, protocols, and change control procedures.
- d. Applying approved patches and modifications in accordance with Postal Service policies and procedures.
- e. Implementing appropriate security administration and ensuring logon IDs are unique and passwords comply with standards.
- f. Setting up and managing accounts in accordance with Postal Service policies and procedures.
- g. Disabling accounts of personnel who have been terminated or transferred and accounts that have been inactive for an extended period of time.
- h. Making the final disposition (e.g., deleting) of the accounts and information.
- 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. Maintaining an accurate inventory of Postal Service information resources.
- l. Ensuring the availability of information resources by implementing backup and recovery procedures.
- m. Ensuring audit logs, as appropriate for the specific platform, are implemented, monitored, and protected from unauthorized disclosure or modification and retained for one year or the time directed by the Postal Service Records Officer.
- n. Reviewing audit logs and maintaining records of the reviews.

9-2.8 **Database Administrators**

Database administrators (DBAs) are responsible for the following for information resources under their control:

- a. Implementing appropriate database security based on the platform-specific hardening guidelines.
- b. Implementing information security policies and procedures for all database platforms and monitoring the implementation of database security mechanisms to ensure they are functioning properly and in compliance with established policies.

- c. Applying approved patches and modifications in accordance with Postal Service policies and procedures.
- d. Maintaining an accurate inventory of Postal Service information resources.
- e. Implementing appropriate database security administration and ensuring logon IDs are unique and passwords comply with standards.
- f. Setting up and managing accounts in accordance with Postal Service policies and procedures.
- g. Disabling accounts of personnel who have been terminated or transferred and accounts that have been inactive for an extended period of time.
- h. Making the final disposition (e.g., deleting) of the accounts and information.
- 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. Ensuring the availability of databases by implementing database backup and recovery procedures.
- l. Ensuring logs for databases are turned on, logging appropriate information, protected from unauthorized disclosure or modification, monitored, and retained for one year or the time directed by the Postal Service Records Officer.
- m. Reviewing audit logs and maintaining records of log reviews.
- n. Assisting with periodic reviews, audits, troubleshooting, and investigations as requested.

9-2.9 **All Personnel**

All personnel are responsible for the following:

- a. Performing the security functions and duties associated with their job, including the safeguarding of their logon IDs and passwords.
- b. Changing their password immediately if they suspect the password has been compromised.
- c. Prohibiting any use of their accounts, logon IDs, passwords, PINs, and tokens by another individual.
- d. Complying with appropriate information security policies and procedures.

9-2.10 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 9.2

Security Services Responsibilities

Activity	Mgrs. Comp. ¹	Mgr SIS	Executive Sponsors	All Managers	System/ Database Admins	All Personnel
Request, authorize, & review access authorization.			X	X		
Manage accounts.	X	X			X	
Manage logon IDs.					X	
Protect logon IDs & passwords.						X
Implement secure identification & authentication mechanisms.		X			X	X
Manage remote access.	X	X				
Protect sensitive and critical information.						X
Implement encryption.		X	X			
Prevent data residue.			X		X	
Ensure information resource & data integrity.	X	X	X		X	
Ensure appropriate level of availability.	X	X	X		X	
Implement appropriate security administration & audit logging.					X	

¹Managers, computing operations/infrastructures (e.g., manager, Host Computing Services; manager, Customer Care Operations; and manager, Engineering)

X = Responsible for accomplishment

Other managers with responsibilities for security services include: chief inspector; inspector general; chief information officer/vice president, Information Technology (CIO/VP IT); and manager, Corporate Information Security Office (CISO) (see Appendix A for a consolidated list of roles and responsibilities).

9-3 Security Services Overview

Information security services are those concepts, properties, and processes utilized 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 and only one user or process to enable tracking of all actions of that user or 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 that 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 the stored information.

- g. Availability ensures information resources will be 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.

9-4 Authorization

Authorization is the process of 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, process, etc.) unless authorized by appropriate Postal Service management. Upon employment, personnel will be granted access to a standard baseline suite of information resources and information technology (IT) services.

9-4.1 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.

9-4.1.1 Clearances

For personnel without clearances, access will be restricted to baseline information services (see Section 9-4.2.1). 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.

9-4.1.2 Need to Know

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

9-4.1.3 Separation of Duties

Only authorized personnel will be approved for access to Postal Service information resources. This approval must be specific to individuals' roles and responsibilities in the performance of duties and must specify the type of access (read, write, delete, execute), specific resources and information, and time periods for which the approval is valid. Separation of duties and responsibilities will be considered when defining roles.

9-4.1.4 Least Privilege

For sensitive, critical, and business-controlled information resources, access will be 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, execute, etc.).

9-4.2 Authorization Process

eAccess is the Postal Service application for managing authorization to information resources.

9-4.2.1 Baseline Information Services

The following baseline information services may be authorized for personnel without personnel security clearances.

- a. ACE Active Directory Account.
- b. E-mail access.
- c. Office suite of services.

The following information services are unavailable under baseline access:

- a. Internet or Intranet browser access.
- b. Remote access.
- c. Access to e-mail except within the Postal Service Intranet.

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

Expiration of Baseline Access Authorization

This baseline access must be set to expire every 3 months and must be renewed via eAccess until the user receives the appropriate personnel security clearance.

9-4.2.2 Requesting Authorization

Requests for authorization to access Postal Service information resources (baseline and beyond baseline) are requested via eAccess at <https://eaccess>.

9-4.2.3 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.

9-4.2.4 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.

9-4.2.5 **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.

9-4.2.6 **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.

9-4.2.7 **Revoking Access**

All managers must ensure that access to information resources is immediately revoked for personnel when no longer required because of change in job responsibilities, transfer, or termination (see 6-7). The manager will advise system and/or database administrators as to the final disposition of files and data.

9-4.2.8 **Emergency Access**

In cases where an individual has possession of Postal Service information that is required by his or her manager when the individual is unavailable, the following process must be followed:

- a. The individual's manager initiates a request for access to the information utilizing a documented procedure (e.g., remedy or info ticket). The individual's manager will be held accountable for this emergency access.
- b. Audit logging for all activities related to this emergency access request is required and must be protected and saved according to the standards described in Section 10-8, *Audit Logs*.
- c. This 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 this emergency access.
- d. The system administrator will either rewrite the access rules giving the manager or the manager's designee access to the information (files) or the system administrator will be authorized by the manager to access that information on the manager's behalf.

- e. Upon completion of the emergency access, all access to the information will be returned to the original state.
- f. The unavailable individual will be notified of the emergency access as soon as he or she becomes available.

9-4.3 **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, such as workstations, consoles, terminals, and any 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.

9-5 **Accountability**

9-5.1 **Description**

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.

9-5.2 **Types of Accountability**

Accountability for access to information resources must be established at the site, network, and the individual level.

9-5.2.1 **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) and restricted by system hardware or software to a unique system, network, or terminal address in a controlled environment.

9-5.2.2 **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.

9-5.2.3 **Individual Accountability**

Individual accountability associates each user or information resource (such as 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 (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:

- 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 (user ID or logon ID).

9-5.3 **Types of Accounts**

Access to information resources will be managed through the use of multiple types of accounts, including the following:

- a. Regular.
- b. Privileged.
- c. Managed.
 - (1) Shared.
 - (2) Training.
 - (3) Machine.
- d. Generic.
- e. Guest.
- f. Other.

9-5.3.1 **Regular Accounts**

Regular accounts provide personnel with the minimum level of information resources and system functionality needed to perform their duties and do not carry special privileges above those required to perform the business function (see 9-4.1.4, Least Privilege). The manager or executive sponsor must authorize the establishment of regular accounts.

9-5.3.2 Privileged Accounts

Privileged accounts provide higher levels of access for individuals who perform system administration and user account maintenance functions or who administer restricted information resources such as databases. Privileged accounts will be used in accordance with the following:

- a. Assignment must be restricted to personnel whose duties require additional privileges.
- b. Privileged accounts must be assigned to a unique individual.
- c. Use is restricted to performing those job functions required by the privileged account; individuals must use their regular user accounts to perform nonprivileged functions.
- d. The number of privileged accounts for any information resource must be kept to a minimum.
- e. An audit trail must be maintained on all privileged account usage (see 9-12, Audit Logging).

9-5.3.3 Managed Accounts

Managed accounts are accounts in which a Postal Service entity is responsible for the lifecycle of the account from creation, deployment, usage, and retirement when no longer needed. Managed accounts must be assigned to the organization's incumbent manager.

9-5.3.3.1 Shared Accounts

Shared accounts have a single logon ID and are used by more than one person. Establishment of shared accounts will meet the following criteria:

- a. Shared accounts must be placed under management control.
- b. The requesting manager is responsible for the use of shared accounts.
- c. The requesting manager must control access to the password.
- d. If accountability is required, such as with privileged documents, the use of this account must be logged.

9-5.3.3.2 Training Accounts

Training accounts are variants of individual or shared accounts that are established on a specific information resource for student use while in class. Training accounts must be limited to the minimum functionality required to achieve the training and must not include access to Postal Service production systems.

9-5.3.3.3 Machine Accounts

Machine accounts are assigned to an information resource or other automated process used to 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. System administrators are responsible for the management and integrity of these accounts.

9-5.3.4 Generic Accounts

Generic accounts are used where accountability is not required. Use of generic accounts must be approved by the manager, CISO.

9-5.3.5 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 utilizes either no password or a widely known password. Guest accounts incorporated into any software or established through any other means must be deleted or disabled.

9-5.3.6 Other Accounts

Standards must be established for other types of accounts, such as started tasks.

9-5.4 Account Management

Accounts must be established in a manner that ensures access is granted on a need to know and least privilege basis.

9-5.4.1 Establishing Accounts

To establish an account, all personnel must follow the process described in 9-4.2.

9-5.4.2 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.

9-5.4.3 Configuring Account Time-outs

Accounts must be configured to log the workstation off the network after a predetermined period of inactivity. This requirement should be automated where possible. The Postal Service default standard period of inactivity is 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.

9-5.4.4 Departing Personnel

Accounts must be deleted or passwords changed when personnel leave the organization.

9-5.5 Handling Compromised Accounts

All personnel who suspect an account has been compromised must immediately notify management and follow the incident reporting process (see Chapter 13).

9-6 Identification

Identification is the process of associating a person or information resource with a unique (enterprise-wide) identifier, such as 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) environments are defined by Engineering.

9-6.1 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 will be issued a logon ID in conjunction with the authorization process (see 9-4.2). No two users will be assigned the same logon ID except those using shared accounts (see 9-5.3.3.1).

9-6.2 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.

9-6.3 Suspending Logon IDs

After six unsuccessful attempts to log on to an information resource, the logon ID or account must be suspended. A user having a computer logon ID suspended must call the Help Desk and follow defined procedures for resolution. Computer logon IDs must be suspended if not utilized for a preset period of time not to exceed 180 days.

9-6.4 Failed Logon Attempts

9-6.4.1 Recording Failed Logon Attempts

Failed logon attempts must be recorded for audit trail and incident reporting purposes.

9-6.4.2 **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.

9-6.5 **Terminating Logon IDs**

Logon IDs not used for a year must be deleted.

9-6.6 **Identification Requirements**

Information resources must comply with security requirements including, but not limited to, the following:

- a. The information resource must, at a minimum, utilize 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. The information resource must not provide any process to bypass the authentication information for any logon ID.
- e. 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."

9-7 **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 environments are defined by Engineering. Means of authentication, or authenticators, may include the following:

- a. Passwords.
- b. PINs.
- c. Shared secrets.
- d. Digital certificates.

- e. Smart cards and tokens.
- f. Biometric devices.

9-7.1 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.

9-7.1.1 Password Selection Requirements

Passwords are intended to be difficult to guess or to crack, using brute force or trial-and-error methods. Information resources that require passwords must be configured to accept only those passwords that meet Postal Service requirements. Password requirements must comply with the following:

- a. For privileged users, personnel in technology areas, mobile users, and personnel using Encryption File System (EFS), 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 (special characters such as &, #, and \$).
- b. For all other 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 (special characters such as &, #, and \$).
- c. For all users, passwords must not contain the user’s name or any part of the user’s full name and must not be one of the past four passwords used for the account.
- d. Passwords must not be repeated (reused) for at least 5 generations.

9-7.1.2 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, street name, etc.).
- 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, or run-on multi-word strings).

9-7.1.3 Initial Password

Passwords must always be delivered in a secure manner. The initial password for users must be sent via First Class Mail, an encrypted delivery system, or personal delivery to the user. Passwords for privileged accounts must be hand-delivered. 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 re-setting forgotten passwords.

9-7.1.4 Password Suspension

After six unsuccessful attempts, suspend the password and disable the account.

9-7.1.5 Re-set Passwords

Users with nonprivileged accounts who have forgotten their passwords or whose accounts have been disabled due to using an incorrect password after six attempts, may re-set their password by invoking ePassword Reset. ePassword Reset will re-set the password to a temporary password and the user must then change the password at first logon.

ePassword Reset is not used for system administrators, database administrators, or other privileged accounts. When privileged users request the re-set of a password, the user must be prepared to provide some predetermined shared secret that only the user would know for validation purposes (see 9-7.3, Shared Secret). Re-set passwords for privileged users must be hand-delivered. The password is re-set to a temporary password and the user must then change the password at first logon.

9-7.1.6 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 re-set the account. Password expiration requirements are as follows:

- a. Prior to the expiration of authentication information such as passwords, the information resource will provide notification to the user.
- b. At least every 30 days, passwords for privileged accounts or for those accounts considered sensitive (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.

9-7.1.7 Requests for Use of Non-Expiring Password Accounts

All requests for use of non-expiring password accounts must be submitted in writing (e-mail is acceptable) by the executive sponsor to the manager, CISO. These accounts will be tracked for compliance purposes. The executive sponsor will be held accountable for the usage of these accounts. If approval is granted, the following compensating controls must be implemented:

- a. Account must be in Active Directory. (The only exception will be source-restricted mainframe accounts.) No privileged access allowed.
- b. Non-expiring accounts must be requested and documented through eAccess.
- c. Source restrict the account to a specific host and do not allow console or remote entry.
- d. Encrypt the LDAP call to keep the password from being transmitted across the network in clear text.
- e. Use a maximum length complex password.
- f. Strictly restrict access to the password to operations staff with a need to know.
- g. Change password when personnel with access to the account leave or transfer.

9-7.1.8 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 (see 9-5.3.3.1, Shared Accounts).
- b. Passwords must not be written down.
- c. Aside from initial password assignment and password re-set 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.

9-7.1.9 Password Storage

Passwords must be stored in an encrypted format. This includes passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems.

9-7.1.10 Vendor Default Passwords

All vendor-supplied default 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.

9-7.1.11 **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. Suspend password and disable account after an administrator-configurable number of unsuccessful entries.
- c. Require re-authentication by the user, as well as re-confirmation of the new password, at the time of an attempted password change.
- d. Store passwords in a one-way encrypted format.
- e. Encrypt passwords in transmissions.

9-7.2 **Personal Identification Numbers**

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.

9-7.2.1 **PIN Generation and Selection**

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 such as social security number, telephone number, or house address.

9-7.2.2 **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.

9-7.2.3 **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

9-7.2.4 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 (see 9-7.3). All forgotten PINs must be replaced with new PINs, which must be securely delivered.

9-7.2.5 PIN 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 (see 9-7.2.2).

9-7.2.6 PIN Cancellation and Destruction

A PIN suspected of compromise must be cancelled immediately and a new PIN generated and delivered via secure methods (see 9-7.2.2). 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.

9-7.2.7 PINs Used for Financial Transactions

PINs used for financial transactions must comply with American National Standards Institute (ANSI) 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.

9-7.3 Shared Secret

A shared secret is an authentication mechanism used to re-set a user's password or PIN. When requesting the re-set 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 utilizing shared secrets provides a secure process for recording an initial shared secret and changing the shared secret in the event of suspected compromise.

9-7.4 Digital Certificates and Signatures

9-7.4.1 Digital Certificates

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 utilized (see 9-7.4.3).

9-7.4.2 Digital Signatures

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.

9-7.4.3 Certificate and Signature Standards

Standards for digital certificate properties, utilization, and acceptance can be found in Handbook AS-600, *United States Postal Service Certification Practice Statement*. Standards established for the use, maintenance, and performance of cryptographic keys associated with digital certificates and signatures can be found in section 9-8.4, *Key Management*.

9-7.5 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, will set 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.

9-7.6 Biometrics

Biometric information is a valid method of authentication. Biometrics are technologies used to authenticate individuals by means of unchanging biological characteristics, such as 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 information and must be protected. The CISO, in conjunction with the Inspection Service, will set standards for the use of biometric authentication and the storage of biometric information.

9-7.7 **Nonrepudiation and Strong Authentication**

9-7.7.1 **Nonrepudiation**

Nonrepudiation is the security property that assures 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.

9-7.7.2 **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.

9-7.7.3 **Strong Authentication**

Strong authentication consists of two-factor or multi-factor authentication tools, such as a 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.

9-7.8 **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.

9-7.9 **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.

9-7.9.1 **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.

9-7.9.2 **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, SIS), 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 will require 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.

9-7.9.3 **Time-out Requirements (Re-authentication)**

The inactivity time-out standard for Postal Service information resources is 30 minutes. After 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.

9-7.9.3.1 Workstations

The inactivity time-out standard for all Postal Service workstations is 30 minutes. After 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.

9-7.9.3.2 Applications

The inactivity time-out standard for all application sessions must be set at a minimum of 30 minutes, unless business and operational necessities dictate an extension on the period of inactivity. The business and operational needs and the risks associated with any extension of the 30-minute standard must be reviewed, approved, and documented in the ISA process.

9-7.9.3.3 Remote Access

For remote access, the communications session will be limited to 2 hours. After 2 hours, the workstation will be disconnected from the network. The normal workstation inactivity time-out standard described above applies.

9-7.9.4 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.

9-7.10 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.

9-8 Confidentiality

9-8.1 Description

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 will be 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.

9-8.2 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 or business-controlled sensitivity information must have the capability to encrypt information. 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.

9-8.2.1 Required for Transmission and Storage on Removable Devices and Media

Information resources storing or processing sensitive or business-controlled sensitivity information must implement approved encryption based on Postal Service encryption and key recovery policies. Encryption must be used for sensitive and business-controlled sensitive information that is transmitted or stored on removable devices or media. Encryption must be used for payment card industry (PCI) information throughout the lifecycle. Encryption must also be used for sensitive and business-controlled sensitive information that is stored off Postal Service premises.

9-8.2.2 Recommended for Storage on Non-Removable Devices

Additionally, encryption is recommended for sensitive and business-controlled sensitive information stored on non-removable devices. See 3-5.4, *Encryption of Information*.

9-8.3 Utilization of Encryption Products

Encryption products must comply with requirements including, but not limited to, the following:

- a. Information resources using encryption must utilize 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.

9-8.4 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.

9-8.4.1 Protecting Encryption Keys

Encryption keys must be treated as sensitive 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 utilized, the key must be stored in such a way that it cannot be retrieved in clear text.

9-8.4.2 Recommended 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.

9-8.4.3 **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.

9-8.5 **Elimination of Residual Data**

The information resource must have the capability to ensure that there is no residual data exposed to unauthorized users (see 3-6.2, Removal of Data Residue).

9-9 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.

9-9.1 **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 environment 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 guidelines 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.

9-9.2 Data Integrity

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.

9-10 Availability

Availability is the security property that ensures information resources will be accessible by authorized personnel or information resources when required.

Availability is maintained through comprehensive and interrelated efforts that include, but are not limited to, the following:

- a. Business continuity and contingency planning (see Chapter 12).
- b. Capacity planning and scalability.
- c. Redundancy.
- d. Secure backup and recovery.
- e. High availability.

9-10.1 **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, scalable information resources should be considered that require little or no change to the configuration or the application when adding hardware or data storage.

9-10.2 **Redundancy**

Redundant systems for servers and firewalls may be recommended where warranted to ensure the availability of critical and business-controlled criticality information resources. The implementation of redundant systems should be based on a cost benefit analysis and the recovery time objective (RTO).

9-10.3 **Secure Backup and Recovery**

All information resources must have the capability to perform secure backups and recovery. The information resource must have the capability to check the integrity of data read from a backup file when performing a restore function (see 12-8, Backup of Information Resources).

9-10.4 **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. Offsite vaulting of application transactions.
- e. 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.

9-11 Security Administration

Security administration includes management constraints, operational procedures, and supplemental controls established to protect information resources. Sensitive, critical, and business-controlled information resources must implement logical access security.

9-11.1 Security Administration Requirements

Security administration functions that must be implemented for USPS 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.

9-11.2 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. Guidelines on consistent and effective use of security features, including their interaction and how to generate a new security configuration.
- d. Guidelines 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.

9-12 Audit Logging

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred. Audit logs include system logs, event logs, error logs, and Web logs. Information resources must implement audit logging functions including, but not limited to, 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.

9-12.1 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. Protecting the audit log and its control mechanisms from modification, deletion, or disabling of the function.
- f. Generating real-time alarms of operational problems (e.g., running out of storage space) and audit log malfunctions.
- g. Providing authorized individuals with access to enable retrieval, printing, and archiving (copying to long-term storage devices) of audit log contents.
- h. Providing administrators with audit analysis tools to selectively retrieve records from the audit log to produce reports, establish audit trails, and perform other related functions.

9-12.2 **Audit Log Events**

The information resource must log security events including, but not limited to, the following:

- 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. Use of privileged accounts.
- f. Creation, storage, or revocation of keying material.
- g. Shutdowns, restarts, and backups.
- h. Installation and updates of software.
- i. Access to audit logs.
- j. Changes to logs.

9-12.3 **Audit Log Contents**

The information resource must record event information including, but not limited to, the following:

- 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.

9-12.4 **Audit Log Protection**

Secure audit logs so they cannot be altered, by:

- a. Limiting the viewing of logs to those with job-related need.
- b. Protecting audit log files from unauthorized modifications.
- c. Promptly backing-up audit log files to a centralized server or media that is difficult to alter.
- d. Using file integrity monitoring and change detection software on logs to ensure existing log data cannot be changed without generating alerts.

9-12.5 Audit Log Reviews

System administrators and database administrators must review audit logs regularly (see 10-8) and maintain a record of the review.

9-12.6 Audit Log Retention

Audit logs, whether in electronic or nonelectronic format, must be retained for one year or as directed by the Postal Service Records Office (see Handbook AS-353).

This page intentionally left blank

10 Hardware and Software Security

10-1 Policy

The Postal Service will 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. Change control procedures, virus protection procedures, and standard configurations of hardware and software must be implemented to reduce Postal Service exposure to unnecessary risks and vulnerabilities.

10-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for hardware and software security are defined in the sections below and are depicted in [Exhibit 10.2](#).

10-2.1 Chief Inspector

The chief inspector is responsible for the following:

- a. Ensuring the physical security of facilities containing Postal Service computing equipment.
- b. Conducting site security reviews to ensure the physical security of Postal Service information resources.
- c. 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.

10-2.2 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Providing guidance and oversight on the security of hardware, software, and applications.
- b. Providing guidance and oversight for security architecture, technologies, and controls.
- c. Establishing evaluation criteria and recommending security hardware, software, and audit tools.
- d. Recommending changes to configurations that would minimize or mitigate security threats to information resources.
- e. Assessing and ensuring compliance with information hardware and software security policies through inspections, reviews, and evaluations.

10-2.3 **Managers, Computing Operations/Infrastructures**

The managers, computing operations/infrastructures (e.g., manager, Host Computing Services; manager, Customer Care Operations; manager, Engineering), are responsible for the following in the mainframe, distributed, and engineering environments:

- a. Implementing and maintaining security throughout the mainframe, distributed, and engineering infrastructures.
- b. Coordinating and implementing standard configurations for mainframe, distributed, and engineering devices.
- c. Recommending and deploying hardware and software based on the Postal Service security architecture.
- 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 software to scan for malicious code and usage of nonstandard network protocols.
- f. Implementing information security policies, procedures, and hardening standards for mainframe, distributed, and engineering information resources.
- g. Maintaining the integrity of data and information resources and ensuring the appropriate level of information resource availability.
- h. Implementing appropriate security administration and ensuring accounts are managed appropriately.

10-2.4 **Manager, Secure Infrastructure Services**

The manager, Secure Infrastructure Services (SIS), is responsible for implementing and maintaining a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.

10-2.5 **Executive Sponsors**

Executive sponsors are responsible for the following for the information resources under their control or sponsorship:

- a. Maintaining an accurate inventory of Postal Service information resources and coordinating hardware and software upgrades.
- b. Implementing configuration management for information resources.
- c. Ensuring hardware, software, and application security through the implementation of appropriate controls.
- d. Ensuring software is licensed and information resources under their control are obtained according to official Postal Service processes.
- e. Ensuring compliance with information security policies and procedures.

10-2.6 **Installation Heads**

Installation heads are responsible for the following:

- a. Maintaining an accurate inventory of Postal Service information resources at their facility.
- b. Implementing hardware security.
- c. Implementing configuration management for information resources.
- d. Ensuring that the Postal Service security policy, guidelines, and procedures are followed in all activities related to information resources at their facility, including procurement, development, and operation.

10-2.7 **System Administrators**

System administrators, including computer system administrators, network administrators, and firewall administrators, are responsible for:

- a. Implementing information security policies and procedures for all information resources under their control and monitoring the implementation for proper functioning of security mechanisms.
- b. Implementing appropriate platform security based on the platform-specific hardening guidelines 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 Postal Service policies and procedures.
- e. Implementing appropriate security administration and ensuring logon IDs are unique.
- f. Testing information resources to ensure security mechanisms are functioning properly.
- g. Tracking hardware and software vulnerabilities.
- h. Maintaining an accurate inventory of Postal Service information resources under their control.

- i. Maintaining a record of monitoring activities for information resources under their control.
- j. Assisting with periodic reviews, audits, troubleshooting, and investigations as requested.
- k. Ensuring virus protection software and signature files are updated and kept current for resources under their control.

10-2.8 **Database Administrators**

Database administrators (DBAs) are responsible for:

- a. Implementing appropriate database security based on the platform-specific hardening guidelines for the information resources under their control.
- b. Monitoring the implementation of database security mechanisms to ensure they are functioning properly and in compliance with established policies.
- c. Testing applications to ensure security mechanisms are functioning properly.
- d. Tracking hardware and software vulnerabilities, and deploying database security patches.
- e. Tracking hardware and software vulnerabilities.
- f. Maintaining an accurate inventory of Postal Service information resources under their control.
- g. Maintaining a record of monitoring activities.
- h. Assisting with periodic reviews, audits, troubleshooting, and investigations as requested.

10-2.9 **All Personnel**

All personnel are responsible for the following:

- a. Complying with applicable laws, regulations, and Postal Service information security policies and procedures.
- b. Using licensed and approved hardware and software.
- c. Protecting and securing all information resources assigned to them whether fixed or portable.
- d. Maintaining an accurate inventory of Postal Service information resources under their control.
- e. Protecting against viruses and malicious code.

10-2.10 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for audits, evaluations, and reviews of Postal Service programs and operations.

Exhibit 10.2

Hardware and Software Security Responsibilities

Activity	Mgrs. Comp ¹	Mgr SIS	CISO	Executive Sponsors	Installation Heads	System/ Database Admins	All Personnel
Secure the Postal Service computing infrastructure.		X	C				
Use licensed & approved hardware & software.			C				X
Test hardware & software, track hardware & software vulnerabilities.	X	X	C			X	
Maintain information resource inventories.	X	X	C	X	X	X	X
Implement configuration management.	X	X	C	X	X	X	
Implement hardware security.	X	X	C	X	X	X	X
Implement software and application security, protect against viruses and malicious code.	X	X	C	X		X	X

¹Managers, computing operations/infrastructures (e.g., manager, Host Computing Services; manager, Customer Care Operations; manager, Engineering)

X = Responsible for accomplishment

C = Consulting support as required

Other managers with responsibilities for hardware and software security include: chief inspector and inspector general (see Appendix A for a consolidated list of roles and responsibilities).

10-3 General Guidelines for Hardware and Software

10-3.1 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, Secure Infrastructure Services (SIS), is responsible for implementing and maintaining a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.

10-3.2 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 Infrastructure Toolkit (ITK). Personnel wishing to use information resources not on the ITK must obtain approval from the Enterprise Architecture Committee (EAC).

Engineering must approve hardware and software used within the mail processing and mail handling equipment (MPE/MHE) environment.

10-3.3 **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 (see Chapter 8).

10-3.4 **Tracking Hardware and Software Vulnerabilities**

Vulnerabilities in hardware and software platforms must be reviewed on a regular basis. All vulnerability advisories involving the software and hardware in use within the Postal Service information resources must be tracked. Designated personnel in Customer Care Operations, Host Computing Services, Secure Infrastructure Services, and Engineering must be on software and hardware vendor advisory mailing lists and other forums appropriate to the information resources under their control.

10-3.5 **Maintaining Inventory**

All personnel are responsible for maintaining an accurate inventory 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.

10-3.6 **Licensing Hardware and Software**

Computer hardware and software purchased for the Postal Service must be registered or licensed to the Postal Service.

10-3.7 **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, sniffers) must be used only by authorized personnel for approved purposes (see Chapter 14, Compliance and Monitoring).

10-4 **Configuration and Change Management**

10-4.1 **Scope**

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 (see the Postal Service national change and configuration management process at <http://blue.usps.gov/changemgmt>).

10-4.2 **Configuration Control**

To effectively manage information resources, initial or baseline configurations of the information resources must be established prior to deployment. Configurations of information resources must be periodically reviewed to identify new vulnerabilities and security requirements.

10-4.3 **Standard Configurations**

Standard configurations of hardware and software 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.

10-4.4 **Change/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. All changes must be appropriately approved and documented. Change control records must be maintained to support and document system software maintenance, software and hardware upgrades, and any local system modifications.

10-4.5 **Patch Management**

An effective patch management process must be implemented to investigate, prioritize, test, track, and control the deployment and maintenance of software releases, and to resolve known security vulnerabilities. The patch management process must be addressed by all information resources installed in the Postal Computing Environment. 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: maintaining current knowledge of available patches; deciding what patches are appropriate for particular information resources; prioritizing the patches to be installed; testing patches in a nonproduction environment first in order to check for unwanted or unforeseen side effects; developing a backout plan, which includes backing up the systems about to be patched to be sure that it is possible to return to a known-good working configuration should something go wrong with the patch; ensuring that patches are installed properly; testing information resources after installation; and 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 OS 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, etc.).

10-4.6 **Significant Changes**

Significant changes to sensitive, critical, and business-controlled information resources will require the re-initiation of the Information Security Assurance (ISA) process (see 8-5).

10-4.6.1 **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.

10-4.6.2 **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.

10-4.7 **Change Management for Pilots and Proofs of Concept**

Pilots and proofs of concept must be subject to the same change control requirements as production systems. The executive sponsor must ensure that change control procedures are followed during testing and implementation. Change control for pilots and proofs of concept for mail processing and mail handling equipment environments are defined by Engineering.

10-5 **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.

10-5.1 **Mainframes**

Appropriate security controls must be enabled. For mainframe implementation of this security policy, contact the manager, Host Computing Services.

10-5.2 **Network Devices**

Appropriate security controls must be enabled on all network devices, including routers, hubs, and switches (see Chapter 11, Networks and Communications).

10-5.3 **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 guidelines unique to the individual server platform. Implement only one primary function per server or blade (e.g., Web server, database server, and domain name server [DNS] should be implemented on separate servers). Configuration standards for servers in the MPE/MHE environments are defined by Engineering.

10-5.3.1 **Hardening Servers**

All information resources must be implemented on servers hardened to Postal Service standards. Hardening control standards must be implemented

specific to each platform. These standards must be updated as new vulnerabilities are uncovered and updates are available. Servers must not be deployed to a production environment prior to hardening.

Note: The manager, SIS, is responsible for the distribution of server hardening standards.

10-5.3.2 **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, SIS.

10-5.3.3 **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 section 10-5.3.4 for an exception). Database servers located inside Postal Service firewalls must not be directly accessible from Web servers or other systems located outside firewalls. Database servers must not be deployed to a production environment before hardening.

10-5.3.4 **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 or critical.
- b. Application is not Internet accessible.
- c. Application is not on the DMZ.
- d. Application is not enclaved with 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.

10-5.4 **Hardening Servers**

All workstations must have appropriate security controls. All personnel are responsible for protecting the information resources at their individual workstations and abiding by all information security policies and procedures that apply to their individual environment.

All Postal Service workstations 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 workstation to receive these patches and pattern updates is required.

Disable unnecessary services and protocols. Remove unnecessary functions such as scripts, drivers, features, subsystems, and file systems. Personnel that fail to connect their workstations to the Intranet in 30 days will be locked out and the user will need to call the IT Help Desk to be reinstated.

10-5.4.1 **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 key, and desk-fastening security equipment.

10-5.4.2 **Password- or Token-Protected Screen Saver**

Where feasible, all workstations 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.

10-5.5 **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, critical, or business-controlled information stored on them. In addition, sensitive and business-controlled sensitivity information on 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.

10-6 **Software and Applications Security**

Security attributes and capabilities must be a 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.

10-6.1 **Software Safeguards**

Software configuration and installation must include only the features and functions necessary to perform the required business activities. Precautions must include, but are not limited to, the following:

- a. Activating or enabling all safeguards embedded in computer software and protecting these safeguards against compromise, subversion, or unauthorized manipulation.
- b. Disabling or removing all features and files that have no demonstrable purpose.
- c. Disabling or removing default privileged logon IDs, changing all default passwords, and removing guest accounts.
- d. Prohibiting use of administrative and root accounts for running production applications.
- e. Limiting access to the specific files required.
- f. Restricting access to systems software utilities to a small number of authorized users.

10-6.2 **Secure Transaction Compliance**

10-6.2.1 **Financial Requirements**

Financial requirements must be implemented when processing e-Commerce financial transactions (these requirements are set by dominant financial institutions, such as banks and VISA).

10-6.2.2 **Health Insurance Portability and Accountability Act Requirements**

Health Insurance Portability and Accountability Act (HIPAA) requirements must be implemented when processing health or medical information.

10-6.3 **Version Control**

All software that can be modified must be managed through the authorized Postal Service change control and management process (see 10-4, 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.

10-6.3.1 **Updating Software**

Only authorized personnel may perform updates to the production application programs or operating system libraries/directories.

10-6.3.2 **Distributing Software**

Controls must be in place to regulate and manage the distribution of Postal Service system-wide 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.

10-6.3.3 **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 ITK must be directed to the Enterprise Architecture Committee (EAC) (see 5-5.1, Acquiring Hardware and Software).

10-6.3.4 **Unapproved Software**

Unapproved software will be removed by the IT staff.

10-6.4 **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.

10-6.5 **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 (see Chapter 8). Application software developed in house or outsourced for sensitive, critical, or business-controlled information resources must undergo the Information Security Assurance (ISA) process.

10-6.6 **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.

10-6.6.1 **DBMS Activity Logs**

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 (see Chapter 12, Business Continuance Management).

10-6.6.2 **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, critical, and business-controlled information and enforce need to know.

10-6.6.7 **COTS Software**

Commercial-off-the-shelf (COTS) software must be acquired and distributed 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 environment will be approved by Engineering.

10-6.6.8 **COTS Vulnerability Assessment**

A COTS software security evaluation must be performed for all proposed additions to the postal computing environment. It is recommended that the COTS vulnerability assessment be updated for sensitive, critical, and business-controlled information resources.

10-6.6.9 **Independent Code Review**

Custom programs or COTS applications that contain custom programming or scripts may be subject to an independent code review. The independent code review will review the source code and documentation to verify compliance with software design documentation and programming standards and to ensure the absence of malicious code (see 8-6.3.6, Conduct Independent Security Code Review).

10-6.6.10 **Browser Software**

Workstations should use the 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.

10-6.6.11 **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.

10-6.11.1 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.

10-6.11.2 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.

10-6.11.3 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.

10-7 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 (boot sector, file infector, multipartite, link, stealth, macro, e-mail, blended), worms, keystroke loggers, botnets, Trojans, trap doors, time bombs, activity trackers, remote control agents, snoopware, spyware, and adware.

10-7.1 Virus Protection Software**10-7.1.1 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.

10-7.1.2 Scanning

To ensure Postal Service perimeter security, Security Information Services will conduct scans for malicious code on the firewalls, FTP servers, mail servers, Intranet servers, Internet application protocols, and other information resources as necessary.

10-7.1.3 Updating

Centralization of automatic updates to virus software is key 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.

10-7.2 **Other Protection Measures**

10-7.2.1 **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.

10-7.2.2 **Evaluating Active Content or CGI Code**

A code review must be conducted on sensitive and critical information resources that contain active content code or CGI scripts. A code review is recommended for business-controlled information resources that contain active content code or CGI scripts. 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 8-6.3.6).

10-7.2.3 **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.

10-7.2.4 **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 will be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems (see Chapter 12).

10-7.2.5 **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.

10-7.2.6 **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 anti-spyware 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.

10-8 Audit Logs

Audit logs must record events and situations including, but not limited to, the following:

- a. Significant operation-related activities.
- b. Security-related events.

10-8.1 General Guidelines

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred (see 9-12, Audit Logging). For events where immediate attention is required, the audit utility may trigger alarms that are directed to the proper location for action.

10-8.2 Protection of Audit Logs

Audit logs must be treated as "RESTRICTED INFORMATION"; protected from unauthorized access, modification, or destruction; and reviewed periodically for action. Access to logs must be granted based upon need to know and least privilege. Audit logs must be backed up and stored offsite.

10-8.3 Retention of Audit Logs

Audit logs must be retained for one year or as directed by the Postal Service Records Office.

10-8.4 Review of Audit Logs

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. In this process, audit logs may also support the recovery of data lost or modified.

10-8.5 Operating System Audit Logs

Operating systems must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of system integrity. Operating system software must have an audit capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction.

10-8.6 Application Audit Logs

Critical or sensitive applications that have logging functions, such as database management software used to store information, must implement their logging functions. Business-controlled applications may implement logging when appropriate.

This page intentionally left blank

11 Networks and Communications

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 will safeguard the availability and integrity of the network in accordance with Postal Service policies and procedures.

11-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for networks and communications are defined in the sections below and are depicted in [Exhibit 11.2](#).

11-2.1 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for the following:

- a. Investigating computer intrusions as per the designation of functions between the OIG and the Postal Service Inspection Service.
- b. Conducting independent audits, evaluations, and reviews of Postal Service programs and operations.

11-2.2 **Chief Inspector**

The chief inspector is responsible for ensuring the physical security of facilities containing Postal Service telecommunications equipment. The chief inspector may conduct site security reviews to ensure the physical security of Postal Service telecommunications systems.

11-2.3 Manager, Corporate Information Security Office

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Ensuring the development of appropriate security policy regarding the Postal Service telecommunications network.
- b. Providing guidance and oversight for security architecture, technologies, procedures, and controls.
- c. Approving network services and protocols.
- d. Providing consulting support for securing the network perimeter, infrastructure, integrity controls, asset inventory, identification, authentication, authorization, intrusion detection, penetration testing, and audit logs.
- e. Assessing and ensuring compliance with telecommunications and network security policies through inspections, reviews, and evaluations.
- f. Providing support to the OIG during the conduct of investigative activities concerning information security, the computing infrastructures, and network intrusion as requested.
- g. Providing support to the chief inspector during the conduct of facility/site security reviews as requested.

11-2.4 Manager, Secure Infrastructure Services

The manager, Secure Infrastructure Services (SIS), is responsible for the following:

- a. Implementing and maintaining operational information security throughout the infrastructure.
- b. Managing network addressing and virtual private networks.
- c. Recommending and deploying network hardware and software based on the Postal Service security architecture.
- d. Monitoring and tracking all physical connections between any component of the Postal Service telecommunications infrastructure and monitoring and tracking any other information resource not under Postal Service control.
- e. Ensuring secure and appropriate management of the Postal Service Managed Network Services (MNS).
- f. Implementing security controls and processes that will safeguard the availability and integrity of the MNS.
- g. Determining the standards and configuration for secure enclaves.
- h. Implementing the network perimeter, firewalls, demilitarized zones (DMZs), and enclaves.
- i. Assessing information resources to determine the need for placement in a secure enclave.
- j. Managing a network connectivity review process (see Handbook AS-805-D, *Information Security Network Connectivity Guide*).

- k. Designating the chairperson of the Network Connectivity Review Board (NCRB).
- l. Ensuring secure and appropriate connectivity to the MNS.
- m. Ensuring network services and protocols used by Postal Service information resources provide the appropriate level of security for the MNS.
- n. Implementing secure methods of remote access and appropriate remote access controls.
- o. Implementing strong authentication, digital certificates, digital signatures, biometrics, smart cards, tokens, and the associated infrastructure.
- p. Ensuring that only Postal Service-approved encryption products are used.
- q. Implementing appropriate security administration and managing accounts appropriately.
- r. Maintaining the integrity of data and information resources.
- s. Conducting capacity planning.
- t. Approving network services, protocols, and standard configurations for devices.
- u. Providing security incident detection through perimeter virus scanning and intrusion detection services.
- v. Approving, managing, and ensuring appropriate perimeter virus scanning, penetration testing, and network vulnerability scans and testing.
- w. Ensuring network perimeter security by implementing, approving, and managing firewalls, enclaves, proxy servers, and intrusion detection services.
- x. Managing a computer incident response team (CIRT) to help the Postal Service contain, eradicate, document, and recover following a computer security incident and return to a normal operating state.
- y. Approving the use of networking monitoring tools, except those used by the OIG.

11-2.5 **Manager, Information Security Services**

The manager, Information Security Services (ISS), is responsible for the following:

- a. Designating the ISS representative(s) to the Network Connectivity Review Board.
- b. Providing consulting support regarding physical, administrative, and technical security controls and processes that safeguard the availability and integrity of the Postal Service MNS.
- c. Providing consulting support regarding secure connectivity to the MNS.
- d. Providing support to the CIRT, as requested.
- e. Providing consulting support regarding network services and protocols used by Postal Service information resources.

- f. Providing support to the OIG during the conduct of investigative activities concerning information security, the computing infrastructures, and network intrusion as requested.
- g. Conducting site security reviews as requested.
- h. Providing support to the chief inspector during his or her conduct of site security reviews as requested.

11-2.6 **Executive Sponsors**

Executive sponsors are responsible for the following:

- a. Ensuring appropriate funding for proposed business partner connectivity, including costs associated with the continued support for the life of the connection.
- b. Initiating and complying with the network connectivity request requirements and process as documented in Handbook AS-805-D, *Information Security Network Connectivity Guide*.
- c. Ensuring prompt notification and escalation of any security incident to the CIRT.
- d. Notifying the NCRB when the business partner trading agreement ends or network connectivity is no longer required.

11-2.7 **Installation Heads**

The installation heads are accountable for information, equipment, and systems within their custody. This responsibility includes the following:

- a. Ensuring that the Postal Service security policy, guidelines, and procedures are followed in all facility system activities, including procurement, development, and operation.
- b. Ensuring that all employees who use or are associated with the information resources in the facility are provided security awareness training appropriate to their responsibilities.
- c. Taking appropriate action in response to employees who violate established security policy or procedures.
- d. Cooperating with the Inspection Service to ensure the physical protection of the network infrastructure located at the facility.
- e. Ensuring prompt notification and escalation of any security incident to the CIRT.
- f. Creating and maintaining an accurate inventory of Postal Service network infrastructure components within their custody.

11-2.8 **Network Connectivity Review Board**

The Network Connectivity Review Board (NCRB) is responsible for implementing the network connectivity request process for reviewing, evaluating, and approving network connectivity. The manager, SIS, appoints the chairperson of the NCRB.

11-2.9 **Manager, SIS Threat Assessment and Response**

The manager, SIS Threat Assessment and Response (also known as CIRT), is responsible for the following:

- a. Providing timely and effective response to computer security incidents as they occur.
- b. Working with an affected organization to contain, eradicate, document, and recover following a computer security incident.
- c. Engaging other Postal Service organizations including, but not limited to, the OIG and ISS.
- d. Conducting a post-incident analysis of an incident where appropriate and recommending preventive actions.
- e. Maintaining a repository for documenting and analyzing Postal Service-wide security incidents.
- f. Interfacing with other governmental agencies and private sector computer incident response centers.
- g. Participating in and providing information for Postal Service security awareness.
- h. Developing and documenting CIRT processes for incident reporting and management.

11-2.10 **System Administrators**

System administrators, including network administrators and firewall administrators, are responsible for the following:

- a. Identifying internal and external attacks on Postal Service information resources.
- b. Identifying anomalies regarding Postal Service information resources.
- c. Reporting information security incidents and anomalies to their manager and the CIRT.
- d. Implementing identification, authentication, authorization, and network services in compliance with Postal Service security policies.
- e. Ensuring audit logs, as appropriate for the specific platform, are implemented, monitored, reviewed, and retained for the time period specified by Postal Service security policy.
- f. Monitoring the implementation of network security mechanisms to ensure they are functioning properly and in compliance with established security policies.
- g. Assisting with periodic reviews, audits, troubleshooting, and investigations as requested.

11-2.11 **Business Partners**

Business partners may request connectivity to Postal Service network facilities for legitimate business needs. The Postal Service requires justification for connecting to its network facilities. Business partners requesting or utilizing connectivity to Postal Service network facilities will be responsible for the following:

- a. Initiating a request for connectivity with the Postal executive sponsoring the request.
- b. Complying with Postal Service network connectivity requirements and process.
- c. Abiding by Postal Service information security policies regardless of where the systems are located or who operates them.
- d. Reporting any information security incidents immediately to the CIRT, executive sponsor, and the ISSO assigned to their information resource.
- e. Allowing site security reviews by the Postal Inspection Service or Information Security Services.
- f. Allowing audits by the Postal Service OIG.

11-2.12 **All Personnel**

All personnel are responsible for the following:

- a. Promptly reporting to the CIRT and, as appropriate, to their immediate supervisor, manager, or system administrator any information 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.
- b. Completing Form 1360, *Information Systems Security Incident Report*, and sending it to the CIRT.
- c. Protecting computers and terminals that are connected to the Postal Service network.
- d. Protecting logon IDs and passwords.
- e. Protecting sensitive, critical, and business-controlled information resources.
- f. Complying with Postal Service remote access information security policies, including those for virtual private networks (VPNs), modem access, dial-in access, secure telecommuting, and remote management and maintenance.
- g. Complying with acceptable use policies including electronic mail, electronic mail encryption, and Internet policies.

Exhibit 11.2

Networks and Telecommunications Security Responsibilities

Activity	OIG	CISO	Mgr. SIS	Executive Sponsors	Installation Heads	NCRB	Mgr. Threat Assess.	System Admins	Business Partners
Manage network addressing; establish firewalls, secure enclaves, & DMZs; approve remote management & maintenance.		C	X						
Approve network services and protocols.		X	X						
Secure network perimeter.	C	C	X						
Implement network integrity controls.		C	X			P	P	P	
Protect network infrastructure.	C	C	X	P	P	C	P	P	P
Maintain network asset inventory.			X		P			P	
Implement identification, authentication, & authorization.		C	X	P				X	
Conduct intrusion detection & penetration testing.	X	C	X				C		
Implement security for Internet technologies.		C	X	P	P	P	P	P	P
Monitor network perimeter traffic.	X	C	X						
Request network connectivity.				X		P			X
Approve network connectivity.				P		X			
Manage VPNs.			X						
Manage audit logs.	C	C	X	P				X	P

X = Responsible for accomplishment

P = Participant

C = Consulting support as required

Other managers and personnel with responsibilities for networks and telecommunications security include: chief inspector; manager, Information Security Services (ISS); and all personnel (see Appendix A for a consolidated list of roles and responsibilities).

11-3 Networks and Communications Security

11-3.1 Purpose

Physical, administrative, and technical security controls and processes that safeguard the confidentiality, availability, and integrity of the network will be implemented to:

- 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 equipment security.
- g. Ensure that recovery procedures are in place and working.
- h. Implement appropriate auditing procedures.

11-3.2 Scope

Network and communications security policies apply to the following:

- a. All transmission technologies used on behalf of the Postal Service in Postal Service or non-Postal Service facilities. These technologies include, but are not limited to, 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 multi-media communications, regardless of transmission technology.

11-4 Network Architecture

Network architecture describes the appearance, functions, locations, and resources used in the network infrastructure. Network architectures must be designed with the appropriate level of administrative and technical security controls. The Postal Service protects its network architecture through the following:

- a. Managing network addresses.
- b. Approving services and protocols.
- c. Securing network perimeters.
- d. Implementing network integrity controls.

11-4.1 **Managing Network Addressing**

All network names and addresses must be managed and approved by a central addressing authority within Secure Infrastructure Services (SIS). Internal network addresses must be protected, and access to internal network addresses will be based upon need to know and least privilege. When appropriate, SIS will conceal network addresses and provide translation of nonroutable addresses.

11-4.2 **Approving 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 MNS into the remote site are as follows:

- a. All connections to any network(s) other than the MNS must be controlled by firewalls managed by Postal Service SIS or SIS designee.
- b. Network changes to the agreed upon configuration must be approved by SIS. Changes are made if the network is not managed under the Postal Service MNS contract.
- c. SIS or SIS designee must have:
 - (1) Unrestricted physical access to the network.
 - (2) Unrestricted network access to perform network level intrusion detection.
 - (3) Unrestricted network access to perform network and host security vulnerability and penetration testing, and unrestricted access to other network auditing functions deemed necessary by SIS.
- d. All equipment connected to the network must meet current Postal Service security hardening standards.
- e. Connections to the MNS must be firewalled in a manner similar to current Postal Service secure enclave firewalling.
- f. Business partner connections, including those that are an extension of the MNS, must be Postal Service-managed via firewall or other network filtering device.
- g. Passwords used to manage systems on the network must not be used to manage other systems or networks.
- h. All remote site systems administrators must have a Postal Service security clearance.

11-4.3 **Securing 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, SIS, 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 utilized, as approved by the manager, SIS.

Note: The Inspection Service manages, secures, monitors, scans, and supports its own network and information technology (IT) infrastructure. The Inspection Service network connectivity to the MNS must comply with the requirements and processes for approved connectivity to the MNS.

11-4.4 **Implementing Network Integrity Controls**

The manager, SIS, must establish 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.

11-5 **Protecting the Network Infrastructure**

11-5.1 **Scope**

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 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. Conducting intrusion detection.
- j. Conducting penetration testing.
- k. Conducting vulnerability scans.

11-5.2 **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 only those personnel with a demonstrated need for access (see Chapter 7).

11-5.3 **Maintaining Network Asset Control**

All infrastructure components must be inventoried at regular intervals and labeled for asset management and physical protection (see Chapter 10).

11-5.4 **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 "RESTRICTED INFORMATION." Access to network configuration information must be based upon the security principles of need to know and least privilege.

11-5.5 **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 (see Chapter 9).

11-5.6 **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 (see Chapter 9).

11-5.7 **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, SIS, is responsible for the distribution of information resource hardening standards.

11-5.8 **Determining When a Secure Enclave Is Required**

Information resources designated as sensitive or critical must be assessed by the manager, SIS, to determine if the resource should reside in a secure enclave. It may be recommended that certain business-controlled information resources also be assessed for inclusion in a secure enclave. A completed business impact assessment (BIA) and the architectural diagram must be submitted to the manager, SIS, for review and determination of enclave requirements.

11-5.9 **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 pre-defined, securable information traffic flows.
- f. Restrict administration to a small, well-defined set of system administrators.
- g. Employ intrusion detection systems.
- h. Audit the network boundary controls through the performance of network scanning procedures on a regular basis.

11-5.10 **Isolation of Postal Service and Non-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. Non-publicly available Postal Service information must be isolated from non-Postal Service information (e.g., business partner and vendor information) in transit.

11-5.11 **Scanning, Penetration Testing, and Vulnerability Assessments**

Only personnel authorized by the CISO will 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 Inspection Service has the authority to scan and conduct penetration testing and vulnerability assessments on their own network and information technology (IT) infrastructure.

11-5.11.1 **Conducting Intrusion Detection**

Requests for intrusion detection must be directed to the manager, CISO, for approval. Intrusion detection will be conducted for Postal Service networks by SIS or the CISO designee. The OIG conducts intrusion detection at their discretion.

11-5.11.2 Conducting Penetration Testing

Requests for penetration testing must be directed to the manager, CISO, for approval. Penetration testing will be conducted for Postal Service networks by SIS or the CISO designee. The OIG conducts penetration testing on Postal Service networks at its discretion.

11-5.11.3 Conducting Vulnerability Scans

Requests for vulnerability scans must be directed to the manager, CISO, for approval. Vulnerability scans will be conducted on Postal Service information resources by SIS or the CISO designee.

11-6 Internet Technologies

The Postal Service uses Internet technologies in the following environments:

- a. Internet.
- b. Intranet.
- c. Extranet.

11-6.1 Internet

Access to the Internet from Postal Service information resources must be routed through Postal Service-approved access control technology, such as firewalls and filtering routers.

11-6.2 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.

11-6.3 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 Guide*. 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.

11-7 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.

11-7.1 Implementing Internet Security Requirements

Internet-accessible information resources, such as those residing on DMZs, must implement Internet security requirements that include, but are not limited to, the following:

- a. Securely partitioning each Internet accessible environment, such as 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 and business-controlled sensitivity 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.

11-7.2 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.

11-7.2.1 Firewall Configurations

Postal Service firewalls must be configured to:

- 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 going 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 re-boot machines must have the same secure configuration).
- f. Audit and monitor all services, including those not permitted, 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.

11-7.2.2 **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.

11-7.2.3 **Firewall Administration**

All Postal Service firewalls must be located in a controlled environment. Firewall administration must be performed from the local console or via remote access if approved by the manager, SIS, and appropriately secured through strong authentication and encryption. Firewall configurations must be protected and treated as "RESTRICTED INFORMATION." Access to firewall configuration information must be based upon the security principles of need to know and least privilege.

11-7.2.4 **Firewall System Integrity**

Firewall system configuration and integrity must be validated and tested periodically by the firewall administrator.

11-7.2.5 **Firewall Backup**

The firewall (system software, configuration data, database files, etc.) must be backed up as determined in the Business Contingency and Continuity Plan (BCCP).

11-7.3 **Establishing Demilitarized Zones**

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. Web servers and electronic commerce systems accessible to the public must reside within a DMZ with approved access control, such as a firewall or gateway. Sensitive, critical, and business-controlled data must not reside within a DMZ. All inbound traffic to the Intranet from the DMZ must be passed through a proxy-capable device.

11-7.4 **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.

11-8 **Network Connections**

11-8.1 **Establishing Network Connections**

The NCRB must approve in advance the establishment of network connectivity. Any connectivity to the Postal Service network must allow monitoring.

11-8.2 **Requesting Connections**

The NCRB provides the mechanism for requesting, reviewing, evaluating, and approving connectivity between non-USPS individuals and organizations wishing to establish connectivity to the Postal Service Managed Network Services (MNS).

11-8.3 **Approving Connections**

Requests for connectivity to the MNS 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, *Information Security Network Connectivity Guide*.

11-9 **Business Partner Requirements**

Business partners must follow and comply with the requirements identified in Handbook AS-805-D, including, but not limited to, the following:

- a. Initiating requests with the executive sponsor for access to the Postal Service network.
- b. Complying with all Postal Service information security policies.
- c. Allowing site reviews by the Inspection Service or ISS.
- d. Allowing audits by the Office of the Inspector General.
- e. Reporting any security incident immediately to the CIRT and executive sponsor.
- f. Notifying the executive sponsor when connectivity is no longer required.

11-10 **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.

11-11 Implementing Access and Administrative Controls

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.

11-12 Remote Access

Use eAccess to ask your manager for permission to use a workstation or laptop remotely to access the Postal Service Intranet. Protect the remote workstation or laptop so unauthorized personnel cannot gain access to the Intranet. Do not use personal information resources to connect to the Postal Service Intranet.

11-12.1 Authentication

Where remote access is required, all information resources must implement remote access security. Information resources should be capable of strong authentication on application or network connections requiring remote access. Remote access from a non-Postal Service site requires users or devices to authenticate at the perimeter or connect through a firewall.

Personnel outside Postal Service firewalls must authenticate at the perimeter. In addition, personnel outside Postal Service firewalls must use an encrypted session, such as VPN or secure socket layer (SSL), if transmitting sensitive or business-controlled sensitive information.

11-12.2 Virtual Private Network

A virtual private network (VPN) provides end users with a way to securely access information on the Postal Service network 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 security strategy and 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 Handbook AS-805-D, *Information Security Network Connectivity Guide*.

- 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 SIS.

11-12.3 **Modem Access**

11-12.3.1 **General Modem Access**

Modem access for all information resources to and from Postal Service networks must be approved in writing in advance by the manager, SIS, and must implement the information resource protection measures described below.

Note: Additional modem approval by the manager, SIS, is not required for approved remote access services such as virtual private network (VPN) or point-to-point protocol (PPP).

11-12.3.2 **Requirements for Workstations with Modems**

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 SIS.
- 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.

11-12.4 **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, SIS. All approved dial-in access must be established through Postal Service centralized dial-in services.

11-12.5 **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.

11-12.6 **Remote Management and Maintenance**

If you are not at your own workstation, your access must be encrypted. 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, ISS, and the manager, SIS, in cooperation with the requesting organization.

11-13 Network Audit Logs

Network audit logs must record events and situations including, but not limited to, the following:

- a. Significant operation-related activities.
- b. Security-related events.

11-13.1 **General Guidelines for Network Audit Logs**

Network audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred (see 9-12). For events where immediate attention is required, the audit utility may trigger alarms that are directed to the proper location for action.

11-13.2 **Protection of Network Audit Logs**

Network audit logs must be treated as “RESTRICTED INFORMATION”; protected from unauthorized access, modification, or destruction; and reviewed periodically for action. Access to logs must be granted based upon need to know and least privilege. Audit logs must be backed up and stored offsite.

11-13.3 **Retention of Network Audit Logs**

Audit logs must be retained for one year or as directed by the Postal Service Records Office.

11-13.4 **Review of Network Audit Logs**

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. In this process, audit logs may also support the recovery of lost or modified data.

11-13.5 **Network and Secure Enclave Audit Logs**

Network and secure enclave audit logs must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of network integrity. Network and secure enclave applications must have an audit capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction.

This page intentionally left blank

12 Business Continuity Management

12-1 Policy

The Postal Service, in continuing to meet its business continuity and contingency planning commitments, protect its personnel and assets, and reduce the likelihood and impact of a disruption to essential business functions for both itself and its customers, must implement the Business Continuity Management (BCM) program. BCM is a Postal Service program designed to minimize risk to and provide cost-effective protection for Postal Service assets and to support continuity of business operations and recovery of information technology applications, resources, and services.

12-1.1 Scope

BCM applies to Postal Service information resources and facilities designated by the vice president, Chief Technology Officer (VP/CTO), as major information technology (IT) sites. BCM is not limited to information technology operations or functions.

12-1.2 What BCM Comprises

BCM comprises Business Continuity Planning (BCP), as described in Section 12-4, and Disaster Recovery Planning (DRP), as described in Section 12-5 of this handbook.

Note: Federal agencies and the Postal Service are required to establish and maintain a viable Continuity of Operations Plan (COOP) capability to ensure that essential functions will still be performed during any emergency or situation that might interrupt normal business functions. COOP identifies essential business functions and consists of plans and procedures, alternate facilities, and alternate interoperable communications and data support systems reinforced by comprehensive training, orientation, and exercise programs.

12-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for BCM are defined in the sections below and are depicted in [Exhibit 12.2](#).

12-2.1 Chief Inspector

The chief inspector is responsible for the physical protection of Postal Service facilities, assets, and personnel and for the information security program currently delegated to the VP/CTO.

Note: The Inspection Service has the autonomy to manage its own network and information technology infrastructure.

12-2.2 Vice President, Emergency Preparedness

The vice president, Emergency Preparedness, is responsible for the following:

- a. Developing, implementing, and coordinating emergency preparedness plans to protect Postal Service employees, customers, operations, and the mail during disasters and national emergencies.
- b. Functioning as the Postal Service emergency response coordinator.

12-2.3 Vice President, Chief Technology Officer

The VP/CTO is responsible for the following:

- a. Identifying Postal Service facilities to be designated as major IT sites.
- b. Developing a BCM program for the Postal Service. This responsibility for the BCM program has been delegated to the manager, Corporate Information Security Office.

12-2.4 Manager, Corporate Information Security Office

The manager, Corporate Information Security Office, has delegated the responsibility for defining, planning, developing, implementing, managing, testing, exercising, and monitoring for compliance of a sustainable information technology BCM program for the Postal Service to the manager, BCM.

12-2.5 Manager, Business Continuance Management

The manager, BCM, is responsible for the following:

- a. Defining, planning, developing, implementing, managing, testing, exercising, and monitoring for compliance of a sustainable BCM program for the Postal Service.
- b. Ensuring that appropriate business continuity plans (which includes the incident management team, facility recovery, and workgroup recovery) are developed, tested, and exercised for business functions and information technology services.

- c. Ensuring appropriate application disaster recovery plans (ADRP) are developed and tested for all critical and business-controlled criticality information resources that support critical business functions and services.
- d. Developing and implementing lines of communication to the CTO organization, executive sponsors, and business units, and providing consulting services concerning matters of BCM.
- e. Providing BCM awareness and training for Postal Service personnel.
- f. Ensuring compliance with BCM and information security policies.
- g. Providing disaster recovery (DR) services and processes that enhance the ability of the Postal Service to reduce interruptions to IT services at major IT sites.

12-2.6 **Managers of Major Information Technology Sites**

Managers of major IT sites are responsible for the following:

- a. Functioning as the Incident Management Team (IMT) leader for their respective facilities.
- b. Identifying and training key technical personnel to provide support for the BCP and the DRP for their respective facilities and information resources housed in their facilities and at the alternate DR facilities.

12-2.7 **Manager, Telecommunications Services**

The manager, Telecommunications Services, is responsible for the following:

- a. Ensuring that recovery plans and sufficient capacity are in place for the recovery of the telecommunications infrastructure for the IT-supported Postal Service sites.
- b. Identifying and training key technical personnel to provide support in the BCP and the DRP for information resources housed in IT-supported Postal Service sites.

12-2.8 **Managers of Development Centers**

Managers of development centers are responsible for the following:

- a. Providing support services to the executive sponsor through the appropriate portfolio manager for all matters relating to BCM.
- b. Ensuring the development of ADPAs for applications developed at their respective sites or applications developed under their governance and ensuring that those ADPAs are tested in accordance with their application's designated criticality.
- c. Identifying and training key technical personnel to provide support in the exercise or testing of BCP plans for their respective facilities and ADPAs for applications developed at their sites, applications developed under their governance, and applications housed at their sites or alternate site facilities.

- d. Identifying and training alternate technical personnel to support critical and business-controlled criticality applications in case of disaster.

12-2.9 **Information Systems Security Officers**

Information systems security officers (ISSOs) are responsible for the following:

- a. Conducting a business impact assessment (BIA) on each information resource.
- b. Ensuring that the sensitivity and criticality designations and recovery time objectives (RTOs) are properly recorded in the Enterprise Information Repository (EIR).

12-2.10 **Portfolio Managers**

Portfolio managers are responsible for the following:

- a. Providing coordination and support to executive sponsors for all matters relating to DR processes, e.g., coordination and support for DR costing models.
- b. Functioning as the liaison between executive sponsors and DR service providers in planning and executing DR requirements.

12-2.11 **Executive Sponsors**

Executive sponsors are responsible for the following:

- a. Identifying essential business functions that support the mission of the Postal Service and determining the applications that are required to support these essential business functions.
- b. Ensuring the implementation of appropriate backup and backup verification of applications.
- c. Developing an ADRP for critical and business-controlled critical applications.
- d. Funding application recovery (including, but not limited to, hardware/software licenses required, ADRP development, testing, and maintenance) for applications.

12-2.12 **All Managers**

Managers at all levels are responsible for the following:

- a. Ensuring the development, exercise, and maintenance of all BCP plans and ensuring that those plans are exercised yearly.
- b. Planning for the resumption of normal business functions when notified that their facility can be safely occupied again.
- c. Complying with emergency preparedness policies and processes.
- d. Participating in BCM awareness and training activities, testing, and exercises.

- e. Ensuring that their personnel participate in BCM awareness and training activities, testing, and exercising.
- f. Providing the funding, people (e.g., site facility recovery team manager, application testers), and time necessary to develop, exercise, and maintain the BCP and DRP plans.
- g. Ensuring the development, testing, and maintenance of all ADRPs and ensuring that those plans are tested as designated by their criticality.
- h. Ensuring that information resources under their control are available and that appropriate backups are maintained.
- i. Ensuring that operational workarounds for essential components of information resources under their control are developed, tested, and maintained for use in the event the RTO cannot be met.

Exhibit 12.2

Business Continuity Management Responsibilities

Activity	Executive Sponsors	Portfolio Managers	All Managers	Managers of Major Information Technology Sites	Managers of Development Centers	ISSOs	BCM Manager
Develop, maintain, and exercise IMT plans				X/F			C
Develop, maintain, and exercise FRPs				X/F			C
Develop, maintain, and exercise WRPs				X/F			C
Develop, maintain, and test ADRPs	X/F	L		C	X		X
Certify ADRP testing	X/F	L			X		X
Backup applications	X/F	L		X	X		C
Backup information resources other than applications			X/F				C
Develop & maintain operational workarounds (where necessary)	X/F	L					C
Develop, maintain, and exercise COOP plans			X/F				C
Ensure EIR is updated with application criticality & RTO					C	X	C

X = Responsible for accomplishment
 F = Responsible for funding
 L = Liaison and coordinating support as required
 C = Consulting support as required

12-3 Business Continuance Management

The BCM processes include, but are not limited to, the following:

- a. Business continuity planning.
- b. Disaster recovery planning.
- c. Relationship of criticality and RTO.
- d. Recovery testing for IT facilities.
- e. Backup of information resources.
- f. Operational workarounds.

12-4 Business Continuity Planning

BCP ensures a comprehensive business recovery strategy for Postal Service information technology sites through the development, implementation, exercising, and maintenance of emergency response and business continuity plans. BCP is implemented for business units, business functions, and facilities.

12-4.1 Scope

Postal Service facilities designated by the VP/CTO as major information technology sites must implement a comprehensive business recovery strategy consisting of three major components: an Incident Management Team (IMT) plan, a facility recovery plan (FRP), and a workgroup recovery plan (WRP) for business units housed at the site.

12-4.2 Business Continuity Planning Software

The Postal Service uses a BCP Web-based planning tool for developing recovery plans and providing a central recovery plan repository. The designated Postal Service BCP software will be used to develop and maintain IMT plans, FRPs, and WRPs.

12-4.3 Business Continuity Plan Requirements

All business continuity plans (IMT Plan, FRP, and WRP), whether for natural disasters, man-made hazards, or work stoppages, must do the following:

- a. Define essential business functions to be performed if operations are partially or completely shut down.
- b. Contain personnel contact information and incident notification procedures.
- c. Be maintained in the designated plan repository. (A hard copy must be stored at an accessible off-site location or in a fireproof container.)
- d. Be protected as restricted information. (This requirement applies to all copies.)
- e. Provide plan access to all individuals who have a need to know.

- f. Be reviewed and updated as necessary at least every 6 months.
- g. Be exercised yearly. The goal of the yearly exercise should be to test both the accuracy and completeness of the documentation as well as the reasonableness of the plan.
- h. Be revised in response to the Lessons Learned Report issued following an exercise.

12-4.4 **Business Continuity Plans**

12-4.4.1 **Incident Management Team Plan**

An IMT plan must be developed for all Postal Service facilities designated by the VP/CTO as major information technology sites. The plan directs the management of the crisis.

The IMT plan designates an alternate site for the relocation of IMT members. From this location, the IMT will direct all emergency management functions during and following the emergency event. This site is not intended to function as an alternate facility for the restoration of critical business functions or as a site to restore information processing for essential business functions.

The designated alternate site is used primarily for evaluation and containment at the affected facility, although it may later serve as the facility from which restoration coordination activities are conducted.

12-4.4.2 **Facility Recovery Plan**

An FRP must be developed for Postal Service facilities designated by the VP/CTO as major information technology sites. The FRPs ensure that facility damage is appropriately assessed and repaired and that the resumption of business functions occurs safely.

An FRP describes the process of restoring a facility to a condition in which it meets appropriate personnel, business unit, and safety requirements and makes the facility ready to support business functions and programmatic activities. The FRP does not describe or authorize the resumption of business functions or programmatic activities that are to be conducted within the facility.

Each FRP must contain procedures for prioritizing the order of facility recovery, conducting safety reconnaissance, performing condition assessments, completing recovery operations, and determining facility readiness for reoccupancy.

12-4.4.3 **Workgroup Recovery Plan**

WRPs must be developed for essential business functions housed in facilities designated by the VP/CTO as major IT facilities. WRPs define emergency procedures and the minimum acceptable recovery criteria, including hardware, software, and workspace for business units in the facility.

WRPs ensure the performance of essential business functions during any emergency or business interruption. Individual workgroup plans determine

where and how business unit functions will be performed during the business interruption.

The plan must address the resumption of business functions or programmatic activities that are to be conducted by the business unit.

12-5 Disaster Recovery Planning

The DRP for Postal Service information technology operations and applications ensures that the Postal Service will be able to maintain or quickly resume essential information technology functions in the event of an unplanned interruption to normal business processes. DRP provides a comprehensive disaster recovery strategy through the development, implementation, testing, and maintenance of DR solutions and plans.

12-5.1 Scope

The DRP must be implemented for all critical and business-controlled criticality information resources.

12-5.2 Application Disaster Recovery Plan

An ADRP addresses the requirements for restoring the application at a facility other than the primary facility.

12-5.2.1 Application Disaster Recovery Plan Templates

ADRP templates are available on the IT Web site, under *Support and Disaster Recovery Services*.

- a. The ADRP test must be certified by the development organization, the executive sponsor, and the BCM manager.
- b. At the completion of the ADRP testing cycle, the ADRP test completion date must be documented in the EIR.
- c. ADRPs for critical and business-controlled criticality applications must be tested within 180 days of going into production.
- d. Critical applications must complete a fully operational recovery test of the ADRP every 18 months.
- e. Business-controlled criticality applications must complete either a tabletop walkthrough to test the application or an operational recovery test of the ADRP every 36 months.
- f. ADRPs must be stored in the designated plan repository.
- g. A hard copy of each ADRP must be securely stored off-site with the facility recovery plan of the facility where the application is housed.
- h. All copies of ADRPs must be protected as restricted information.

12-5.2.2 **Application Disaster Recovery Plan Requirements**

ADRP's must meet the following requirements:

- a. An ADRP must be developed, tested, and maintained for critical and business-controlled criticality applications.
- b. Completed ADRPs must be reviewed and accepted by Business Continuity Management before testing can be scheduled.
- c. The ADRP completion date and the scheduled ADRP test date must be documented in the EIR.

12-6 **Relationship of Criticality, Recovery Time Objective, and Recovery Point Objective**

The criticality of an application is determined during the Application BIA, and the EIR is updated at the completion of the BIA process. The RTO, which is the maximum allowable downtime for an application, is determined for applications designated as critical or business-controlled critical. It is how long it takes to restore the application. 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 application, 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. A better RPO requires more frequent backup and transport of the backups offsite or mirroring of the application at an offsite location.

The DR service provider uses the EIR to identify which applications require the development and testing of an ADRP.

12-7 **Mainframe Recovery Testing for Computer Operations Service Centers**

Full recovery testing of mainframe applications for the IT Computer Operations Service Centers located at San Mateo, California, and Eagan, Minnesota, is required every 36 months. Testing requirements for critical and business-controlled criticality applications are unchanged by this requirement.

12-8 Backup of Information Resources

All information resources must implement backup procedures. The responsible Postal Service manager must define the appropriate backup media and frequency.

However, applications determined by the BIA to be critical or business-controlled criticality must implement backup and recovery strategies sufficient to meet the RTO and data currency requirements.

12-8.1 What to Back Up

All essential components of an information resource required for continued operations must be backed up. Backups will 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.

12-8.2 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.

12-8.3 Backup Inventory

An inventory of critical and business-controlled criticality applications backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off-site or stored 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.

12-8.4 Backup Storage Requirements

Backup media must be stored in a secure location (such as a locked cabinet or room with controlled access).

12-8.5 Off-Site Backup Storage Requirements

Backup media for critical and business-controlled 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.

12-8.6 Backup Verification

Backup media for critical and business-controlled criticality 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.

12-8.7 Backup Disposal

All unneeded electronic backup media or hardware containing sensitive and business-controlled sensitivity electronic media must be erased using a method that complies with the most current Postal Service policy and processes on the disposal of sensitive and business-controlled sensitivity media.

12-9 BCM Plan Maintenance and Testing Requirements Summary

Plans/ Applications	Maintenance	Testing
IMT Plan	Reviewed and updated every 6 months	Yearly exercise
FRP	Reviewed and updated every 6 months	Yearly exercise
WRP	Reviewed and updated every 6 months	Yearly exercise
ADRP	Reviewed and updated every 6 months	For critical applications, full operational recovery test within 180 days of going into production and every 18 months thereafter For business-controlled criticality applications, full operational recovery test within 180 days of going into production and either a table top walk through exercise or a full operational recovery test every 36 months thereafter
IT Mainframe Applications @ San Mateo and Eagan	Covered by ADRP	Full recovery test every 36 months

12-10 Operational Workarounds

For essential components of an information resource, operational workaround procedures should be developed (where possible) for use whenever the RTO cannot be met for recovery of the application or information resource. If implemented, these manual workaround procedures will be sustained until the essential components are fully restored at the host facility.

12-11 Continuity of Operations Planning

It is the policy of the Postal Service to respond quickly at all levels in the event of an emergency or threat, including human, natural, technological, and other emergencies or threats, to continue critical operations. Each Postal Service organizational element must be prepared to continue to function and to resume critical operations efficiently and effectively if they are interrupted.

We must plan for meeting the demands of a wide spectrum of emergency scenarios to ensure the continuance and uninterrupted delivery of critical services to the public, other federal agencies, tenants, clients, and employees. Continuity of operations planning must be maintained at a high level of readiness, be capable of being activated both with and without warning, achieve operational status no later than 12 hours after activation, and maintain sustained operations for up to 30 days or until termination. COOP plans must be stored in the Postal Emergency Management System (PEMS). Contact the Office of Emergency Preparedness for additional information on COOP plans.

Each facility designated by the VP/CTO as a major information technology site must include COOP plan requirements in their IMT and FRP to provide the processes and guidance to ensure the safety of personnel and the continuance of critical operations in the event of an emergency or threat of an emergency.

13 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. All information security incidents must be reported in accordance with the policies and procedures provided below regardless of whether or not damage appears to have been incurred.

13-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for incident management are defined in the sections below and are depicted in [Exhibit 13.2](#).

13-2.1 **Inspector General**

The inspector general, Office of the Inspector General (OIG), is responsible for the following:

- a. Conducting independent financial audits and evaluations 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. Investigating computer intrusions as per the designation of functions between the OIG and the Postal Service Inspection Service.
- d. Funding CISO investigative efforts outside of those normally required.

13-2.2 **Manager, Office of the Inspector General, Computer Crimes Unit**

The manager, Office of the Inspector General (OIG), Computer Crimes Unit (CCU), is responsible for the following:

- a. Functioning as an ongoing liaison with the Computer Incident Response Team (CIRT).
- b. Serving as a point of contact between the CIRT and law enforcement agencies.

- c. Conducting criminal investigations of attacks upon Postal Service networks and computers.

13-2.3 **Chief Inspector**

The chief inspector, Postal Inspection Service, is responsible for the following:

- a. Providing physical protection and incident containment assistance during the investigation of information security incidents, as appropriate.
- b. Investigating reported violations of security regulations.
- c. Conducting revenue/financial investigations of such crimes as theft, embezzlement, or fraudulent activity.
- d. Investigating information security incidents, as appropriate.
- e. Funding CISO investigative effort outside of that normally required.

13-2.4 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Ensuring that a process for managing information security incidents is implemented.
- b. Escalating information security incidents to executive management as appropriate.
- c. Ensuring that lessons learned from information security incidents are incorporated into ongoing computer security awareness and training programs.
- d. Providing support to the OIG and the Inspection Service as requested.
- e. Assessing and ensuring compliance with information security incident management policies through inspections, reviews, and evaluations.

13-2.5 **Managers Responsible for Computing Operations and the Advanced Computing Environment Infrastructure**

The managers responsible for computing operations and the advanced computing environment (ACE) infrastructure are responsible for the following:

- a. Creating and maintaining a timely patch management process.
- b. Deploying patches to resources under their control.
- c. Protecting information resources at risk during security incidents, if feasible.
- d. Implementing virus containment.
- e. Providing guidance and education on virus response.
- f. Assisting in restoring information resources following a virus attack.

- g. Reporting suspected information security incidents to the CIRT in a timely manner.
- h. Deploying anti-virus software and updates, as required.
- i. Deploying anti-virus pattern file updates, as required.
- j. Disseminating security awareness and warning advisories to local users.
- k. Ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.

13-2.6 **Program Manager, Secure Infrastructure Services**

The program manager, Secure Infrastructure Services (SIS), is responsible for the following:

- a. Providing security incident detection through perimeter virus scanning and intrusion detection services.
- b. Approving, managing, and ensuring appropriate perimeter virus scanning, penetration testing, and network vulnerability scans and testing.
- c. Managing the CIRT to assist the Postal Service to contain, eradicate, document, and recover following a computer security incident, and return to a normal operating state.
- d. Implementing necessary corrective measures learned from incidents or from other sources.
- e. Providing network intrusion detection services (IDS).
- f. Providing network vulnerability testing and analysis services.

13-2.7 **Computer Incident Response Team**

The CIRT is responsible for the following:

- a. Providing timely and effective response to computer security incidents as they occur based on an established priority for handling incidents.
- b. Working with an affected organization to contain, eradicate, document, and recover following a computer security incident.
- c. Engaging other Postal Service organizations including, but not limited to, the OIG and Inspection Service.
- d. Escalating information security issues up the management chain, as required.
- e. Conducting a post-incident analysis, where appropriate, and recommending preventive actions.
- f. Maintaining a system for tracking incidents until they are closed.
- g. Maintaining a repository for documenting and analyzing Postal Service-wide security incidents.
- h. Interfacing with other governmental agencies and private sector computer incident response organizations.

- i. Participating in and providing information for Postal Service security awareness.
- j. Providing support to the OIG and the Inspection Service, as requested.

13-2.8 **Manager, Telecommunications Services**

The manager, Telecommunications Services, is responsible for the following:

- a. Conducting perimeter scanning for viruses, malicious code, and usage of nonstandard network protocols and immediately reporting suspected information security incidents to the CIRT.
- b. Monitoring network traffic for anomalies and immediately reporting anomalies to the CIRT.
- c. Protecting information resources at risk during security incidents, if feasible.
- d. Providing support to the CIRT for incident containment and response, as requested.
- e. Ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.

13-2.9 **Executive Sponsors**

Executive sponsors are responsible for the following:

- a. Reporting suspected information security incidents to the CIRT in a timely manner.
- b. Protecting information resources at risk during security incidents, if feasible.
- c. Assisting in the containment of security incidents, as required.
- d. Following contingency plans for disruptive incidents.
- e. Assessing damage caused by the incident and taking corrective and preventive measures.
- f. Documenting conversations and actions taken to handle the incident.
- g. Ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- h. Providing resources to correct the damage and remove the vulnerability identified by the incident.

13-2.10 **All Managers**

Managers at all levels are responsible for the following:

- a. Reporting suspected information security incidents to the CIRT in a timely manner.
- b. Protecting information resources at risk during security incidents, if feasible.
- c. Assisting in the containment of security incidents, as directed by the CIRT.

- d. Following contingency plans for disruptive incidents.
- e. Assessing damage caused by the incident and taking appropriate corrective and preventive measures.
- f. Documenting conversations and actions taken to handle the incident.
- g. Ensuring the completion of PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- h. Participating on calls to the CIRT or designating a responsible party to call in.

13-2.11 **Security Control Officers**

Security control officers (SCOs) are responsible for the following:

- a. Reporting suspected information security incidents to the CIRT in a timely manner.
- b. Providing support to the CIRT for incident containment and response as requested.
- c. Ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- d. Responding to physical security incidents.
- e. Reporting physical security incidents to the Inspection Service.
- f. Interfacing with CIRT, Inspection Service, ISS, or OIG, as required.

13-2.12 **System Administrators**

System administrators, including network, firewall, and database administrators, are responsible for the following:

- a. Reviewing audit and operational logs and maintaining records of the reviews.
- b. Identifying anomalies and possible internal and external attacks on Postal Service information resources and immediately reporting them to the CIRT.
- c. Protecting information resources at risk during information security incidents, if feasible.
- d. Assisting in the containment of security incidents, as required.
- e. Taking action, as directed by the CIRT, to eradicate the incidents and recover from them.
- f. Participating in follow-up calls with the CIRT.
- g. Fixing issues identified following an incident.
- h. Initiating a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- i. Ensuring that security patches and bug fixes are updated and kept current for resources under their control.
- j. Ensuring that virus protection software and signature files are updated and kept current for resources under their control.

13-2.13 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.

13-2.14 All Personnel

All personnel are responsible for the following:

- a. Protecting information resources at risk during security incidents, if feasible.
- b. Calling the appropriate Help Desk for technical assistance for response to suspected virus incidents.
- c. Reporting suspected information security incidents immediately to the CIRT, their immediate supervisor or manager, and system administrator.
- d. 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.
- e. Documenting all conversations and actions regarding the security incident.
- f. Completing PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.

13-2.15 Business Partners

Business partners are responsible for the following:

- a. Protecting information resources at risk during security incidents, if feasible.
- b. Reporting suspected information security incidents promptly to the CIRT, the executive sponsor, and the information systems security officer (ISSO) assigned to their project.
- c. Taking action, as directed by the CIRT, to protect against information security incidents; to contain, eradicate, and document them when they occur; and to recover from them.
- d. Documenting all conversations and actions regarding the security incident.
- e. Completing PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- f. Maintaining information security “best practices” on all information resources connecting to the Postal Service infrastructure to include security patches and anti-virus pattern recognition files.

Exhibit 13.2

Incident Management Responsibilities

Activity	Chief Inspector	All Managers ¹	CISO ²	Technical Resources ³	All Personnel /Business Partners	SCOs	Inspector General
Report incident	I	X	X	X/F	X	X	I/A
Protect information resource	X/I	X	C	X/F	X	X	I/A
Contain incident	X/I	X		X/F	X	X	II/A
Process incident report			X/F				A
Analyze incident reports			X/F				A

¹ Executive sponsors and all managers

² CISO and program manager, SIS

³ Technical Resources: managers, computing operations and ACE infrastructure; manager, Telecommunications Services; and system administrators

- X = Responsible for accomplishment
 F = Responsible for funding
 C = Consulting support as required
 A = Independent audits, evaluations, and reviews
 L = Liaison and coordinating support as required

Other managers and organizations with responsibilities for incident management include: CIRT; OIG-CCU; business partners; and managers, Help Desks (see Appendix A, Consolidated Roles and Responsibilities, for details).

13-3 Information Security Incidents

13-3.1 Overview

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, CISO, may get involved at any point on any level for information security related incidents impacting the Postal Service.

13-3.2 Reportable Incidents

Reportable 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 it resides.
- d. Unauthorized activity or transmissions using Postal Service information resources.
- e. Internal or external intrusions or interference with Postal Service networks, such as 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, such as e-mail transmissions, that start without user input.
- k. Files being modified, though no changes in them 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.

13-4 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 and business-controlled sensitive information physically removed from a Postal Service facility.
- i. Encrypt sensitive and business-controlled 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 restricted information, such as 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.

13-5 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 the making of 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, etc.

- d. Conduct penetration testing at times known only to personnel with a need to know.
- e. Regularly review available information sources such as 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.

13-6 Incident Response

13-6.1 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. Corporate Information Security Office (CISO) at 1-919-501-9350.
- e. Security Control Officer (SCO).
- f. Inspection Service.
- g. Office of the Inspector General (OIG) at 1-888-877-7644.

A PS Form 1360 must be completed and submitted to the CIRT. An acceptable facsimile containing the same information required on the form may be submitted.

13-6.2 Information Resource Protection

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:

- 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.

13-6.3 **Incident Containment**

Supervisors or managers who suspect, discover, or are notified of a security-related event must immediately notify the CIRT and initiate appropriate response procedures to contain the incident, protect the confidentiality and integrity of Postal Service information, and ensure business continuity. Appropriate actions following the identification of a security incident include, but are not limited to, the following:

- a. Notifying CIRT for assistance to contain, eradicate, and recover from the security incident.
- b. Notifying the Inspection Service of a physical security incident.
- c. Documenting in a journal or log all conversations and actions taken during the incident handling and response process and making this log available to management personnel on request.
- d. Ensuring personnel follow contingency plans for recovering from disruptive incidents.
- e. Ensuring the completion of a PS Form 1360.

13-6.4 **Processing Incident Reports**

The CIRT is responsible for the following:

- a. Logging and tracking security incident reports.
- b. Ensuring appropriate response and resolution of security incidents.
- c. Engaging appropriate organizational resources, such as the Virus Response Team (VRT), OIG, Inspection Service, etc.
- d. Evaluating and escalating incident reports requiring further action.
- e. Retaining incident reports, supporting evidence, and journals for 1 year or for a time period determined by the OIG.
- f. Providing Inspection Service and OIG access to all reported information security incidents.
- g. Complying with federal sector security incident reporting requirements.

13-6.5 **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.

13-6.6 **Incident Analysis**

The CIRT will analyze security incidents and prepare reports summarizing the causes, frequency, and damage assessments of information security incidents.

CIRT management will analyze the CIRT reports to improve the information security program and keep Postal Service executive management apprised as to the state of information security.

13-6.7 **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.

14 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 to ensure compliance with Postal Service policies, procedures, standards, and guidelines. The activities of any user of 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.

14-2 Roles and Responsibilities

Specific Postal Service roles and responsibilities for compliance and monitoring are defined in the sections below and are depicted in [Exhibit 14.2](#).

14-2.1 **Inspector General**

The inspector general, Office of the Inspector General (OIG), 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. Investigating computer intrusions as per the designation of functions between the OIG and the Postal Service Inspection Service.

14-2.2 **Manager, Office of the Inspector General Computer Intrusion Unit**

The manager, Office of the Inspector General (OIG) Computer Intrusion Unit (CIU) is responsible for the following:

- a. Functioning as an ongoing liaison with the Computer Incident Response Team (CIRT).

- b. Serving as a point of contact between the CIRT and law enforcement agencies.

14-2.3 **Chief Inspector**

The chief inspector, Inspection Service, is responsible for the following:

- a. Conducting site security inspections, reviews, and evaluations of facilities.
- b. Monitoring physical access as deemed necessary.
- c. Monitoring and scanning its own network and information technology (IT) infrastructure.
- d. Assisting the manager, Corporate Information Security Office (CISO), with reviews as appropriate.

14-2.4 **Manager, Corporate Information Security Office**

The manager, Corporate Information Security Office (CISO), is responsible for the following:

- a. Authorizing monitoring and surveillance activities of information resources.
- b. Authorizing (in case of threats to Postal Service infrastructure, network, or operations) appropriate actions that may include viewing and/or disclosing data in order to protect Postal Service resources or the nation's communications infrastructure.
- c. Assessing and ensuring compliance with information security compliance and monitoring policies through inspections, reviews, and evaluations.
- d. Confiscating and removing any information resource suspected of inappropriate use or violation of Postal Service information security policies to preserve evidence that might be utilized in forensic analysis of a security incident.

14-2.5 **Chief Privacy Officer**

The chief privacy officer (CPO) is responsible for the following:

- a. Developing the Postal Service privacy policy.
- b. Developing privacy compliance standards, customer privacy statement, and customer data collection standards, including cookies and web transfer notifications.
- c. Ensuring compliance with privacy regulations and the privacy policy.
- d. Ensuring compliance with the determination of information resource sensitivity policy.
- e. Reviewing and approving in writing requests for message and data content monitoring.

14-2.6 Manager, Secure Infrastructure Services

The manager, Secure Infrastructure Services (SIS), is responsible for the following:

- a. Providing network monitoring and intrusion detection services.
- b. Approving the use of networking monitoring tools, except those used by the OIG.
- c. Ensuring compliance with Postal Service computing infrastructures security standards, processes, and procedures.

14-2.7 Managers, Computing Operations/Infrastructures

The managers, computing operations/infrastructures (e.g., manager, Host Computing Services; manager, Customer Care Operations; manager, Engineering), are responsible for the following:

- a. Installing the authorized internal warning banner in the mainframe, distributed, and engineering computing environments.
- b. Ensuring the compliance with Postal Service information security policy and procedures.

14-2.8 All Managers

Managers at all levels are responsible for the following:

- a. Responding to and becoming compliant with audit findings in their area of responsibility.
- b. Initiating, when required, a written request for message and data content monitoring and sending it to the CPO for approval.
- c. Ensuring the compliance with Postal Service information security policy and procedures.

14-2.9 System Administrators

System administrators are responsible for the following:

- a. Activating audit log features in compliance with Postal Service platform standards.
- b. Maintaining operational logs and records for audit purposes and protecting them from unauthorized disclosure or modification.
- c. Maintaining a record of all monitoring activities for information resources under their control.
- d. Reporting to the computer incident response team (CIRT) any suspicion that information resources have been modified by unauthorized actions.
- e. Ensuring the compliance with Postal Service information security policy and procedures.

Exhibit 14.2

Compliance and Monitoring Responsibilities

Activity	OIG	OIG-CIU	CISO	CPO	Chief Inspector	Mgr. SIS	Mgr. Comp. ¹	All Managers	System Admins
Ensure compliance.			X	X	X	X	X	X	X
Inspect, review, and evaluate.			X/F		X/F	S	S	S	S
Notify users of monitoring.			C				X		
Implement warning banner.			C				X		S
Request monitoring.								X	
Authorize monitoring.			X	X					
Monitor networks.		C	C			X/F			S
Conduct intrusion detection.		X				X/F			
Conduct audits.	X		S			S	S	S	S
Respond to audit.			C	C				X	S

¹Managers, computing operations/infrastructures (e.g., manager, Host Computing Services; manager, Customer Care Operations; manager, Engineering)

X = Responsible for accomplishment

C = Consulting support as required

S = Responsible for support

F = Responsible for funding

(See Appendix A for a consolidated list of roles and responsibilities.)

14-3 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. Inspections, reviews, and evaluations.
- c. Monitoring.
- d. Audits.
- e. Confiscation and removal of information resources.

14-4 Testing Security Systems and Processes

Systems, processes, and custom software must be tested regularly because hackers and others continually discover vulnerabilities, introduced in new software and inadvertently by employees, contractors, and business partners. Test as follows:

- a. 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.

- b. Weekly:
 - Use file integrity monitoring software to alert personnel when files have been modified without authorization. Configure software so it can compare files.
- c. 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).
- d. Annually:
 - Test security controls, limitations, network connections, and restrictions so you know you can identify and stop any attempts at unauthorized access.
 - Test for network-layer penetration (or when infrastructure has been upgraded or modified, i.e. the operating system has been upgraded or a sub-network or Web server has been added).
Test for application-layer penetration (or when an application has been modified).

14-5 Inspections, Reviews, and Evaluations

14-5.1 Requirement

Inspections, reviews, and evaluations must be conducted for information resources and facilities to ensure compliance with Postal Service information security policies.

14-5.2 Information Resources

The CISO will conduct inspections, reviews, and evaluations of information resources:

- a. As part of the Information Security Assurance (ISA) 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 CIO/VP IT as necessary to evaluate the security of information resources.

14-5.3 Facilities

The Inspection Service and/or CISO will conduct inspections, reviews, and evaluations of Postal Service facilities.

14-6 Monitoring

14-6.1 General Monitoring Activities

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 (see 5-3, Monitoring). The Postal Service reserves the right to:

- 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.

Note: “All personnel” includes Postal Service employees, contractors, vendors, business partners, and any other authorized users of Postal Service information systems, applications, telecommunication networks, data, and related resources. It excludes customers whose only access is through publicly available services, such as public web sites of the Postal Service. These customers will only be monitored for site security purposes (see 5-3.1.2, Public Web Site Monitoring).

14-6.2 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).

Note: This monitoring policy does not apply to information resources that are covered by the Postal Service *Internet Privacy Policy Statement* cited below.

14-6.3 Internet Privacy Policy Statement

The Postal Service *Internet Privacy Policy* is available for review at www.usps.com. It restricts Internet monitoring as follows: “For site security

purposes and to ensure that this service remains available to all users ... Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits.”

14-6.4 **User Monitoring Notification**

Where possible, users will be notified by the display of an authorized Postal Service warning banner that the information on Postal Service networks and workstations may be monitored and viewed by authorized personnel, regardless of privacy concerns. This notice must, at a minimum, appear whenever the user first logs on to the system and be included in information security awareness training.

14-6.5 **Warning Banner**

The Postal Service-authorized warning banner must be displayed to users prior to granting session access to Postal Service information resources. 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 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 14.5.4

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.

14-6.6 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. Email and Internet usage.
- e. Message and data content.

14-6.6.1 Requesting User Monitoring

Requests for monitoring network traffic, application and data access, keystrokes and user commands, and email 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 CPO.

14-6.6.2 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 email 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 these monitoring and scanning activities.

The Inspection Service may scan and monitor the Inspection Service network and information technology (IT) infrastructure at its own discretion.

The CPO has the responsibility to authorize, in writing, requests for message and data content monitoring.

In case of threats to Postal Service infrastructure, network, or operations, the manager, CISO, is authorized to take appropriate action, which may include viewing and/or disclosing data in order to protect Postal Service resources or the nation's communications infrastructure.

14-6.7 **Infrastructure Monitoring**

The manager, CISO, is responsible for ensuring security of the Postal Service infrastructure through the following:

- a. Providing security incident detection through perimeter virus scanning and intrusion detection services.
- b. Performing network vulnerability analyses.
- c. Monitoring the Postal Service infrastructure.

14-6.8 **Intrusion Detection**

Intrusion detection devices will be implemented to monitor the infrastructure. The use of all monitoring devices, except those used by SIS or the OIG, must be approved by the manager, CISO. Unauthorized installation and use of monitoring devices is strictly prohibited.

14-7 **Audits**

14-7.1 **Description**

Audits are independent reviews and examinations of records and activities performed to test for adequacy of controls and ensure compliance with established policies and operational procedures. Audits also recommend changes to controls, policies, or procedures. Audits are an effective method for determining the level of protection afforded Postal Service information resources and of uncovering security deficiencies that need to be addressed.

14-7.2 **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.

14-7.3 **Responding to Audits**

Executives responsible for the audited information resource must respond to audit findings and ensure that the information resources under their control comply with Postal Service information security policies and procedures.

14-8 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, will ensure that the chain of evidence (associated with the possession of the confiscated information resource) is preserved and documented.

15 Wireless Networking

15-1 Policy

Wireless devices and the supporting network infrastructure are information resources that must be protected at a level commensurate with their value to the Postal Service. Such protection must include the implementation of controls and processes that address Postal Service information security requirements. Care must be taken when designing and implementing a wireless network.

All 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 NCRB before procurement and integration.

Note: The current effectiveness of the security features of the wireless technologies must be evaluated against the security requirements of the system.

15-2 Roles and Responsibilities

15-2.1 Corporate Information Security Office, Information Technology

The Corporate Information Security Office (CISO), Information Technology (IT), is responsible for the following:

- a. Developing and maintaining wireless information security policies, standards, procedures, and processes.
- b. Approving all wireless connectivity to the Postal Service Intranet via the Network Connectivity Review Board (NCRB).
- c. Providing consulting resources on wireless security issues.
- d. Approving wireless services, protocols, standards, and the use of wireless packet analyzing tools.
- e. Providing wireless security awareness training.

15-2.2 Manager, Telecommunications Services, IT

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

- a. Approving all wireless network infrastructure, including wireless APs and client devices for use within the Postal Service.
- b. Managing, inventorying, tracking, configuring, coordinating, and implementing wireless APs, bridges, and switches.
- c. Approving mail processing equipment/mail handling equipment (MPE/MHE) wireless network infrastructure.
- d. Implementing and maintaining information security throughout the wireless infrastructure.
- e. Negotiating with vendors and procuring all wireless technology except wireless cards/client devices and projects under Engineering contracts in support of MPE/MHE.
- f. Acquiring and implementing tools to monitor wireless infrastructure.
- g. Implementing Postal Service wireless information security policies and procedures.
- h. Ensuring that only authorized personnel (CISO and Office of Inspector General) use wireless packet analyzing tools.
- i. Acting as functional system coordinator for approving wireless access through the Active Directory (AD).

15-2.3 Manager, Distributed Computing Environment, IT

The manager, Distributed Computing Environment (DCE), IT, is responsible for the following:

- a. Controlling placement of approved wireless cards/wireless devices on the ADEPT II Contract.
- b. Managing wireless access through the AD.
- c. Implementing Postal Service wireless information security policies and procedures.

15-2.4 Executive Sponsors

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

- a. Providing resources to ensure security requirements are properly addressed.
- b. Ensuring that all wireless security requirements are included in contracts and strategic alliances.

- c. Ensuring completion of security-related activities throughout the information security assurance (ISA) life cycle.
- d. Funding the deployment and ongoing support of nonstandard wireless local area network (WLAN) implementations.

15-2.5 **Installation Heads**

Installation heads are managers 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. Coordinating with TS/IT to review and approve wireless project plans.
- b. Obtaining NCRB approval for the use of WLAN technology.
- c. Implementing Postal Service wireless information security policy procedures.
- d. Ensuring personnel receive information security training prior to being issued or using wireless technology devices.

15-2.6 **Portfolio Managers, IT**

Portfolio managers, IT, are responsible for the following:

- a. Coordinating preparation of supporting documentation for the use of WLAN technologies with Postal Service applications under their purview.
- b. Ensuring inventory processes are implemented for initiatives under their purview.
- c. Coordinating with TS/IT to review and approve wireless project plans.
- d. Presenting new projects to the NCRB for approval. The manager, Engineering Software Management, or his or her designee, may opt to present MPE/MHE projects to the NCRB for approval.
- e. Ensuring implementation of Postal Service wireless information security policies and procedures.

15-2.7 **Manager, Engineering Software Management, Engineering**

The manager, Engineering Software Management, Engineering, is responsible for the following:

- a. Implementing information security throughout the Engineering wireless infrastructure.
- b. Recommending, coordinating, and implementing standard wireless platform configurations based on TS/IT-approved architecture.
- c. Developing an accurate inventory of MPE/MHE related Postal Service wireless resources, tracking and reacting to security vulnerability alerts, coordinating hardware and software upgrades, and maintaining appropriate configuration management records.

- d. Presenting new MPE/MHE projects to the NCRB for approval.
- e. Negotiating with vendors and procuring TS/IT-approved wireless technology.

15-2.8 **Manager, Maintenance Policies and Procedures, Engineering**

The manager, Maintenance Policies and Procedures, Engineering, is responsible for the following:

- a. Maintaining information security throughout the maintenance wireless infrastructure.
- b. Maintaining standard wireless platform configurations based on the TS/IT-approved architecture.
- c. Maintaining an accurate inventory of MPE/MHE related Postal Service wireless resources and appropriate configuration management records.

15-2.9 **All Managers**

All managers are responsible for the following:

- a. Implementing Postal Service wireless information security policy procedures.
- b. Obtaining NCRB approval for the use of WLAN technology.
- c. Approving wireless access through the eAccess online approval application.
- d. Inventorying and tracking wireless cards/client devices.
- e. Ensuring personnel receive information security training prior to being issued or using wireless technology devices.

15-2.10 **Information Systems Security Officers, IT**

Information systems security officers (ISSOs), IT, are responsible for the following:

- a. Providing consulting support to executive sponsors, portfolio managers, and installation heads regarding the security requirements and controls necessary to protect information resources.
- b. Providing guidance on potential threats and vulnerabilities to information resources, appropriate choice of countermeasures, and the ISA process.
- c. Conducting site security reviews or assisting the Inspection Service in conducting site security reviews.

15-3 **Scope**

This policy applies to all Postal Service functional organizations, employees, contractors, and business partners; information systems; applications; mainframe, mid-range, and windows environments; telecommunications; and

the IT infrastructure, and to all related products developed in-house as well as under contractors.

Note: This policy does not cover wireless devices, such as cellular phones, pagers, etc., unless they transmit data (see MI AS-860-2002-3).

15-4 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 to control and monitor traffic between the wired and wireless segments. See 15-6.2 for the standard architecture for firewall exception.

15-5 Prevention of Unacceptable Risk

Connecting APs or using wireless technology without proper prior approval introduces an unacceptable risk to the Postal Service Intranet and other assets. Non-approved wireless technology must be removed from the Postal Service computing environment.

15-6 Wireless Solutions

15-6.1 **General**

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:

- Standard Wireless Solution
- Nonstandard Wireless Solution

Devices that meet the current WLAN standard solution will not require a firewall between wireless devices and wired networks. All other devices will require a firewall between wireless devices and wired networks.

15-6.2 **Standard Wireless Solution**

15-6.2.1 **General Requirements**

This standard 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 AD credentials.
- d. Mutual authentication of device/client and Remote Authentication Dial-In User Service (RADIUS) server through Postal Service Internal CA Machine Certificates.

15-6.2.2 **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 Certification Authority (CA) machine certificate authenticating to AD.
 - (2) Temporal Key Integrity Protocol (TKIP) encryption.
 - (3) WiFi Protected Access (WPA) for key management.
 - (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 utilizing Postal Service Internal CA certificates.
- f. The 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 WPA 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/IT for use within the Postal Service network.
- l. Service Set Identifier (SSID) standardization must be implemented to support mobility.

15-6.2.3 **How to Request Standard Wireless Services**

Standard wireless connectivity is requested as follows:

Access the NCRB at <http://it>, select Support, CISO Organization Information, Network Connectivity Review Board.

- a. Wireless connectivity must be requested via email to NCRB@email.usps.gov or through the NCRB Web page on the IT Web site. (See Handbook AS-805-D, *Information Security Network Connectivity Process*, for additional information.)
- b. Wireless infrastructure must be requested through TS/IT.
- 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://eaccess>.

15-6.3 **Nonstandard Wireless Solution**

If you are considering a business solution that will include the use of wireless technology that does not meet the standards previously defined, you must do the following:

- a. Obtain NCRB Approval.
Before pursuing a nonstandard wireless technology solution, you must obtain approval to proceed from the NCRB. The NCRB will require a business case for the alternate solution. The NCRB will dictate 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/IT. TS/IT 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) You must next obtain approval of the application, the engineering architecture, and all wireless devices from the NCRB.
 - (a) For implementations involving MPE/MHE:
Contact your responsible design engineering organization who will send an email to NCRB@email.usps.gov or submit a request through the NCRB Web site. Your design engineering organization may also present the MPE/MHE project to the NCRB.
 - (b) For other implementations:
Contact your IT portfolio manager who will send an email to NCRB@email.usps.gov or submit a request through the

NCRB Web page on the IT Web. Your portfolio manager will also act as a presenter to the NCRB on your 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 the wide area network (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/IT.
- 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/IT will arrange for the site survey via the Managed Network Services (MNS) 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. 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/IT, who will then configure the devices. When the devices are programmed they will be sent to the site ready to be installed by the MNS vendor.

15-6.4 **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 (see 15-6.3) as well as the following requirements:

- a. The 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, shared secret) meets our aging and storage requirements, the standard password criteria applies (see Section 9-7, Authentication), 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 or business-controlled sensitivity information is transmitted. Use security mode 3.
- d. The 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.

15-7 Device Support

TS/IT will remotely manage all devices that connect to the network using 802.11x technology. Periodic software updates and product enhancements will be downloaded to APs as required to improve performance and enhance security. Access point management will also include constant operating assessments of the device. Any malfunctions or loss of effectiveness will generate an alert for resolution.

15-8 Procurement Requirements

When considering procurement of wireless hardware, software, and services, meeting the following requirements provides compliance 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 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. Security features including data link-level encryption, 802.1x-compliant authentication model, and regular rotation of encryption keys are built-in.
 - e. Contain secure authorization software/firmware.
 - f. Where Extensible Authentication Protocol (EAP) is used, capable of proper password management (aging, complexity criteria, etc.). The wireless device must have the capability to support password changes in a pre-established timeframe.
 - g. Capable of ensuring 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 minimum standard is 128-bit triple DES (Data Encryption Standard) or AES (Advanced Encryption Standard).
 - l. Capable of providing a secure channel for access point administration.
 - m. Capable of supporting end-to-end cryptographic protection where traffic traverses network segments other than the wireless segment for transmitting sensitive and business-controlled sensitivity information.
 - 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, available in a timely and accurate manner (e.g., remote access for MPI, Structured Wiring switches, and SEF access, etc.).

15-9 Deployment Requirements

It is imperative to carefully plan the deployment of wireless technology. Since it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage through deployment and operation.

Fulfilling the following requirements 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.

15-9.1 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 by 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 service set identifier (SSID), password, read/write community strings, and IP addresses that were 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 and/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 simple theft of equipment is a major 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 wireless local area networks (WLANs).
- x. Install antivirus software as well as 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 or business-controlled sensitivity information on a handheld device. Store sensitive or business-controlled sensitivity 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.

15-9.2 **Physical Security 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 or business-controlled sensitivity 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.

15-9.3 **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; i.e., HTTP, HTTPS, SMTP, etc.
- 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 don’t 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 and business-controlled 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 (WEP) using a 104/128-bit key.
- n. Use a VPN to secure communication between WLAN and LAN resources.

- o. Implement Media 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. Utilize 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 (IV) with sequencing rules, and a re-keying 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 and business-controlled 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.

15-9.4 **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 mandatory access code (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.

- I. When disposing of handheld devices that will no longer be used, sanitize memory to prevent the disclosure of sensitive or business-controlled sensitivity 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.

15-9.5 **Security Requirements for Using a Public Hot Spot**

Personnel connecting to public WLANs in airports, hotels, restaurants, etc., 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 (VPN) to connect back to the Postal Service Intranet, disable split tunneling.
- e. Utilize a personal firewall that detects malicious scanning of your wireless device.

15-10 Compliance and Monitoring Requirements

Security assessments and audits are an essential tool for checking the security posture of a wireless technology and for determining corrective action to make sure 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.

Diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning, sniffers) must be used only by authorized personnel for approved purposes.

I

This page intentionally left blank

Consolidated Roles and Responsibilities

For information on how to contact individuals holding the positions listed below, go to <http://blue.usps.gov/security>.

1 Chief Inspector

The chief inspector is the security officer for the Postal Service and has delegated authority for the information security program to the vice president, Chief Technology Officer. For a complete description of Postal Inspection Service responsibilities, see the *Administrative Support Manual*. The chief inspector is responsible for the following:

- a. Establishing policies and procedures for personnel security, including criteria for clearances and criteria and the identification of sensitive positions.
- b. Determining whether a position is sensitive.
- c. Establishing policies and procedures for physical and environmental security.
- d. Issuing security requirements for personnel, physical, and environmental security.
- e. Conducting background investigations and granting personnel clearances.
- f. Conducting site security reviews, surveys, and investigations of sites to evaluate all aspects of physical, environmental, and personnel security.
- g. Ensuring the physical security of facilities containing Postal Service computer and telecommunications equipment, and monitoring physical access as deemed necessary.
- h. 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 sensitive, critical, and business-controlled media.
- i. Directing the use of the Postal Service Security Force.
- j. 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.

- k. Assisting the manager, Corporate Information Security Office (CISO), with reviews, as appropriate.
- l. Investigating reported violations of security regulations.
- m. Conducting revenue/financial investigations including theft, embezzlement, or fraudulent activity.
- n. Providing physical protection and containment assistance and investigating information security incidents as appropriate.
- o. Funding CISO investigative efforts outside of those normally required.
- p. Managing, securing, scanning, monitoring, and supporting the Inspection Service's own network and information technology (IT) infrastructure.

2 Vice President, Chief Technology Officer

The vice president, Chief Technology Officer (VP/CTO), is responsible for the following:

- a. Ensuring the implementation of information security assurance processes.
- b. Identifying and authorizing baseline information resource services for personnel.
- c. Ensuring that data is assigned to an organizational entity for stewardship.
- d. Ensuring that financial, personnel, and physical resources are available for completing security tasks.
- e. Ensuring the protection and secure implementation of the Postal Service information technology infrastructure.
- f. Together with the vice president of the functional business area, accepting, in writing, residual risk of applications and approving deployment. The VP/CTO has delegated this responsibility to the applicable portfolio manager.

3 Manager, Corporate Information Security Office

The chief inspector has delegated to the VP/CTO responsibility for the information security program. The VP/CTO, in turn, has delegated authority for development, implementation, and management of the information security program to the manager, CISO. The manager, CISO, is responsible for the following:

- a. Setting the overall strategic and operational direction of the Postal Service information security program and its 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, and procedures.
- e. Reviewing the ISA documentation package and accrediting the application.
- f. Managing the network connectivity review process (see Handbook AS-805-D, *Information Security Network Connectivity Process*).
- g. Designating chairpersons for the Network Connectivity Review Board (NCRB) and the Information Security Policy Review Board.
- h. Ensuring secure and appropriate connectivity to the Postal Service intranet.
- i. Conducting site security reviews, as requested, or providing support to the Postal Inspection Service during its site security reviews, as requested.
- j. Providing consulting support regarding physical, administrative, and technical security controls and processes that safeguard the availability and integrity of the Postal Service intranet.
- k. Providing consulting support for securing the network perimeter, infrastructure, integrity controls, asset inventory, identification, authentication, authorization, intrusion detection, penetration testing, and audit logs.
- l. Designating the chairperson of the Network Connectivity Review Board (NCRB).
- m. Providing leadership of the Security Forum for the Enterprise Architecture (EA) Forum.
- n. Developing and implementing a comprehensive information security training and awareness program.
- o. Serving as the central point of contact for all information security issues, and providing overall consultation and advice on information security policies, processes, requirements, controls, services, and issues.
- p. Assessing the adequacy of information security processes in a changing information infrastructure and updating those processes as necessary.
- q. Assessing the adequacy of physical, environmental, and administrative security controls in a changing information technology environment and recommending changes as necessary.
- r. Providing guidance and oversight for information security architecture, technologies, procedures, and controls.
- s. Establishing evaluation criteria and recommending security hardware, software, and audit tools.
- t. Providing guidance and oversight on application security.
- u. Approving the establishment of shared accounts.
- v. Certifying the adequacy of security controls implemented on sensitive, critical, and business-controlled information resources developed for, endorsed by, or operated on behalf of the Postal Service.

- w. Implementing a system for information security incident handling and reporting.
- x. Ensuring that a process for managing information security incidents is implemented.
- y. Incorporating lessons learned from information security incidents into ongoing computer security awareness and training programs.
- z. Ensuring compliance to information security policies through inspections, reviews, and evaluations.
- aa. Providing support to the Office of the Inspector General and the Inspection Service during the conduct of investigative activities concerning information security, the computing infrastructure, and network intrusion, as requested.
- ab. Providing support to the chief inspector during the conduct of facility/site security reviews, as requested.
- ac. Escalating security issues to executive management and promulgating security issues and recommended corrective actions across the Postal Service.
- ad. Authorizing monitoring and surveillance activities of information resources.
- ae. Authorizing (in case of threats to our 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.
- af. 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.
- ag. Reviewing and approving information security policy for mail processing equipment / mail handling equipment.

4 Information Security Executive Council

The Information Security Executive Council consists of appropriate Postal Service representatives and serves as a steering committee advising the CISO on the following:

- a. Prioritizing security issues based on business requirements.
- b. Funding information security programs.
- c. Promulgating information security throughout the Postal Service.

5 Vice Presidents, Functional Business Areas

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

- a. Approving and funding the development of information resources.
- b. Ensuring resources are available for completing information security tasks.
- c. Ensuring the security of all information resources within their organization.
- d. Together with the VP/CTO, 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.
- e. Ensuring that contractual agreements require all contractors, vendors, and business partners to adhere to Postal Service information security policies.

6 Vice President, Emergency Preparedness

The vice president, Emergency Preparedness, is responsible for the following:

- a. Developing, implementing, and coordinating emergency preparedness plans to protect Postal Service employees, customers, operations, and the mail during disasters and national emergencies.
- b. Functioning as the Postal Service Emergency Response Coordinator.

7 Vice President, Engineering

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

8 Vice President, Network Operations Management

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

9 All 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 and ensuring compliance with information security policies by organizations and information resources under their direction.
- b. Ensuring that information security is a part of business decisions.
- c. Promptly elevating problems, requirements, and matters requiring establishment or refinement of information security policies to the level necessary for resolution.
- d. Identifying sensitive information positions in their organizations, ensuring that personnel occupying sensitive positions hold the appropriate level of clearance, and funding background investigations and clearances.
- e. Managing access authorizations and documenting information security responsibilities for all personnel under their supervision.
- f. Ensuring that personnel under their supervision who access information resources receive information security training commensurate with their position and responsibilities, including policies on acceptable use of information resources.
- g. Providing resources, including personnel, financial, and physical assets, to meet information security requirements.
- h. Promulgating information security awareness to all personnel under their supervision, ensuring that their personnel comply with Postal Service information security policies and procedures, and invoking user sanctions as required.
- i. Including employee information security performance in performance evaluations.
- j. Supervising the information security responsibilities of their contractor personnel in the absence of a contracting officer.
- k. Processing departing personnel appropriately and notifying the appropriate system and database administrators when personnel no longer require access to information resources.
- l. Initiating a written request for message and data content monitoring and send to the Chief Privacy Officer (CPO) for approval.
- m. Approving or denying requests, by personnel under their supervision, for access to information resources beyond baseline information resource services and reviewing those access authorizations on a semiannual basis.
- n. Ensuring that all hardware and software are obtained in accordance with official Postal Service processes.
- o. Protecting information resources.

- p. Ensuring the development, exercise, and maintenance of all business continuity planning (BCP) plans and assuring those plans are exercised yearly.
- q. Planning for the resumption of their normal business functions when notified that the facility can be safely occupied.
- r. Complying with emergency preparedness policies and processes.
- s. Participating in and ensuring that their personnel participate in BCM awareness and training, testing, and exercising.
- t. Providing the funding, people (e.g., site facility recovery team manager, application testers), and time necessary to develop, exercise, and maintain the BCP and DRP plans.
- u. Ensuring the development, exercise, and maintenance of all ADPPs and assuring those plans are exercised as designated by their criticality.
- v. Ensuring information resources under their control are available and appropriate backups are maintained.
- w. Ensuring the development, testing, and maintenance of operational workarounds for essential components of an information resource under their control for use in the event that the RTO cannot be met.
- x. Ensuring compliance with Postal Service information security policy and procedures.
- y. Reporting suspected information security incidents to the CIRT in a timely manner, protecting information resources at risk during security incidents, containing the incident, and following contingency plans for disruptive incidents.
- z. Assessing damage caused by the incident and taking appropriate corrective and preventive measures.
- aa. Documenting conversations and actions taken to handle the incident and completing a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- ab. Participating on calls to the CIRT or designating a responsible party to call in.
- ac. Responding to, and complying with, audit findings in their areas of responsibility.

Executive Sponsors

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

- a. Consulting with the Chief Privacy Officer (CPO) on 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.
 - d. Ensuring completion of an information resource risk assessment for all sensitive, critical, and business-controlled information resources under their purview.
 - e. Ensuring completion of a site security review, if the facility hosts a sensitive, critical, or business-controlled information resource.
 - f. Ensuring that contract personnel under their supervision comply with Postal Service information security policies and procedures.
 - g. Ensuring that all information security requirements are included in contracts and strategic alliances.
 - h. Ensuring compliance with, and implementation of, the Postal Service privacy policy, data collection policy, and customer privacy statement.
 - i. Appointing, in writing, an information systems security representative (ISSR).
 - j. Ensuring completion of security-related activities throughout the application ISA life cycle.
 - k. Ensuring that information resources within their purview are capable of enforcing appropriate levels of information security services to assure data integrity.
 - l. Implementing encryption to protect restricted information, as required.
 - m. Preventing residual data from being exposed to unauthorized users as information resources are released or reallocated.
 - n. Authorizing access to the information resources under their control and reviewing those access authorizations on a semiannual basis.
 - o. Ensuring information resource availability through planning for capacity, scalability, and redundancy.
 - p. Maintaining an accurate inventory of Postal Service information resources and coordinating hardware and software upgrades.
 - q. Implementing configuration management for information resources.
 - r. Implementing hardware, software, and application security.
 - s. Ensuring software is licensed and that information resources under their control are obtained in accordance with official Postal Service processes.
 - t. Ensuring appropriate funding for proposed business partner connectivity, including costs associated with the continued support for the life of the connection.
 - u. Initiating and complying with the network connectivity request requirements and process as documented in Handbook AS-805-D, *Information Security Network Connectivity Process*.
 - v. Notifying the NCRB when the business partner trading agreement ends or when network connectivity is no longer required.

- w. Identifying essential business functions that support the mission of the Postal Service and determining the applications that are required to support these essential business functions.
- x. Ensuring the implementation of appropriate backup and backup verification of applications.
- y. Funding application recovery (including but not limited to hardware/software licenses required, ADRP development, testing, and maintenance) for applications.
- z. Protecting information resources.
- aa. Working jointly with the portfolio manager to review the ISA documentation package, accept the residual risk to an application, and approve the application for production or return the application to the applicable lifecycle phase for rework.
- ab. 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 contingency plans for disruptive incidents.
- ac. Assessing damage caused by the incident; documenting conversations and actions taken to handle the incident; completing a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile; and providing resources to correct the damage and remove the vulnerability identified by the incident.

11

Portfolio Managers

Portfolio managers are responsible for the following:

- a. Functioning as the liaison between executive sponsors and IT providers.
- b. Supporting the executive sponsor in the development of information resources and the ISA process, including the BIA, risk assessment, and BCM.
- c. Appointing, if desired, an information systems security representative (ISSR) to perform security-related activities.
- d. Ensuring that the application is entered in the Enterprise Information Repository (EIR) and updated as required.
- e. If a documented vulnerability will not be mitigated, preparing and signing an acceptance of responsibility letter as part of the ISA process.
- f. Providing coordination and support to executive sponsors for all matters relating to disaster recovery (DR) processes, e.g., coordinating and supporting DR costing models.
- g. Functioning as the liaison between executive sponsors and DR service providers in the planning and execution of DR requirements.
- h. Reviewing the ISA documentation package and completing a risk mitigation plan for risks identified as High or Medium.

- i. Working jointly with the executive sponsor to review the ISA documentation package, accept the residual risk to an application, and approve the application for production or return the application to the applicable lifecycle phase for rework.
- j. Ensuring that the application is registered in eAccess.
- k. Accepting personal accountability for adverse consequences if application was placed in production before the Application ISA process was completed.

12 Managers of Major Information Technology Sites

Managers of major information technology sites are responsible for the following:

- a. Functioning as the Incident Management Team (IMT) leader for their facility.
- b. Identifying and training key technical personnel to provide support in BCP and DRP for their facility and information resources housed in their facility and the alternate DR facilities.

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 will be responsible for both 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 sensitive, critical, and business-controlled media.
- 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 ISSO as required, and accepting site residual risk.

- h. Ensuring that the Postal Service security policy, guidelines, 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.
- j. Taking appropriate action in response to employees who violate established security policy or procedures.
- k. Cooperating with the Inspection Service to ensure the physical protection of the network infrastructure located at the facility.
- l. Providing consulting support for information resource backup, providing facility recovery procedures to each of the site's business units, and supporting the development and maintenance of facility recovery plans (FRPs).
- m. Reporting information security incidents to the CIRT in a timely manner, containing the incident, and following contingency plans for disruptive incidents.
- n. Assessing damage caused by the incident, documenting conversations and actions taken to handle the incident, and completing a PS 1360, *Information Security Incident Report*, or an acceptable facsimile.

14 Chief Privacy Officer

The CPO is responsible for the following:

- a. Developing policy relating to defining information sensitivity and determining information sensitivity designations.
- b. Developing policy on Postal Service privacy issues.
- c. Providing guidance to ensure Postal Service compliance with the Privacy Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, and Freedom of Information Act.
- d. Developing privacy compliance standards, customer privacy statement, and customer data collection standards, including cookies and Web transfer notifications.
- e. Approving requests for message and data content monitoring.
- f. Consulting on and reviewing the BIA during and following completion.
- g. Ensuring compliance with the determination of information resource sensitivity policy.
- h. Developing appropriate data record retention, disposal, and release guidelines.

15 Inspector General

The inspector general is responsible for the following (for a description of the Office of Inspector General responsibilities, see *Administrative Support Manual*, Chapter 2):

- 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. Investigating computer intrusions, as per the designation of functions between the OIG and the Postal Service Inspection Service.
- e. Funding CISO investigative efforts outside of those normally required.

16 Manager, Office of the Inspector General, Technical Crimes Unit

The manager, Office of the Inspector General (OIG), Technical Crimes Unit (TCU) is responsible for the following:

- a. Functioning as an ongoing liaison with the CIRT.
- b. Serving as a point of contact between the CIRT and law enforcement agencies.
- c. Conducting criminal investigations of attacks upon Postal Service networks and computers.

17 Manager, Business Continuity Management

The manager, BCM, is responsible for the following:

- a. Defining, planning, developing, implementing, managing, testing, exercising, and monitoring for compliance of a sustainable BCM Program for the Postal Service.
- b. Ensuring that appropriate business continuity plans (Incident Management Team, Facility Recovery, and Workgroup Response) are developed, tested, and exercised for business functions and information technology services.
- c. Ensuring that appropriate ADRPs are developed and tested for all critical and business-controlled criticality information resources that support critical business functions and services.
- d. Developing and implementing lines of communication to the Chief Technology Officer organization, executive sponsors, and business units, and providing consulting services concerning matters of BCM.
- e. Providing BCM awareness and training for Postal Service personnel.

- f. Ensuring compliance with BCM and information security policies.
- g. Providing DR services and processes that enhance the ability of the Postal Service to reduce interruptions to IT services at major IT sites.

18 Manager, Telecommunications Services

The manager, Telecommunications Services, is responsible for the following:

- a. Implementing and maintaining operational information security throughout the infrastructure.
- b. Managing network addressing and virtual private networks (VPNs).
- c. Recommending and deploying network hardware and software based on the Postal Service security architecture.
- d. Monitoring and tracking all physical connections between any component of the Postal Service telecommunications infrastructure and any associated information resource not under Postal Service control.
- e. Ensuring secure and appropriate management of the Postal Service intranet.
- f. Implementing security controls and processes that will safeguard the availability and integrity of the Postal Service intranet and will support the confidentiality of sensitive information.
- g. Implementing the network perimeter, including firewalls, demilitarized zones (DMZs), and secure enclaves.
- h. Implementing secure methods of remote access and appropriate remote access controls.
- i. Implementing strong authentication, digital certificates, digital signatures, biometrics, smart cards, tokens, and the associated infrastructure for network management.
- j. Implementing appropriate security administration and managing accounts appropriately.
- k. Maintaining the integrity of data and network information resources.
- l. Deploying and managing perimeter virus scanning.
- m. Maintaining an accurate inventory of Postal Service network information resources.
- n. Creating and maintaining a timely patch management process for network information resources.
- o. Deploying patches to information resources under his or her control.
- p. Implementing and managing wireless local area networks (WLANs) connectivity.
- q. Conducting capacity planning.
- r. Ensuring that recovery plans and sufficient capacity are in place for the recovery of the telecommunications infrastructure for the IT-supported Postal Service sites.

- s. Identifying and training key technical personnel to provide support in the BCP and DRP for information resources housed in IT-supported Postal Service sites.
- t. Conducting perimeter scanning for viruses, malicious code, and usage of nonstandard network protocols and immediately reporting suspected information security incidents to the CIRT.
- u. Monitoring network traffic for anomalies and immediately reporting anomalies to the CIRT.
- v. Protecting information resources at risk during security incidents, if feasible.
- w. Providing support for CIRT incident containment and response, as requested.
- x. Ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.

19 Managers Responsible for Computing Operations and the ACE Infrastructure

The managers responsible for computing operations and the ACE infrastructure are responsible for the following:

- a. Implementing and maintaining security throughout the mainframe and distributed infrastructure.
- b. Recommending and deploying mainframe and distributed hardware and software based on the Postal Service security architecture.
- c. Coordinating and implementing standard platform configurations based on the Postal Service security architecture.
- d. Creating and maintaining a timely patch management process and deploying patches to resources under their control.
- e. 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.
- f. Implementing information security policies, procedures, and hardening standards.
- g. Defining acceptable thresholds for anti-virus software and recognition patterns.
- h. Deploying and maintaining software to scan for malicious code and usage of nonstandard network protocols.
- i. Functioning as an accreditor for internally managed information resources.
- j. Ensuring that mainframe remote access is appropriately managed.
- k. Implementing appropriate security administration and ensuring that accounts are managed appropriately.

- l. Maintaining the integrity of data and information resources and ensuring the appropriate level of information resource availability.
- m. Ensuring information resource availability through planning for capacity, scalability, and redundancy.
- n. Ensuring the installation of the authorized internal warning banner.
- o. Ensuring the compliance with Postal Service information security policy and procedures.
- p. Protecting information resources at risk during security incidents and implementing virus containment.
- q. Providing guidance and education on virus response.
- r. Assisting in restoring information resources following a virus attack.
- s. Reporting suspected information security incidents to the CIRT in a timely manner.
- t. Distributing anti-virus software and updates, as required.
- u. Distributing anti-virus pattern file updates, as required.
- v. Disseminating security awareness and warning advisories to local users.
- w. Ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.

20 Managers of Development Centers

Managers of development centers shall be responsible for the following:

- a. Providing support services to the executive sponsor through the appropriate portfolio manager for all matters relating to BCM.
- b. Ensuring that ADRPs are developed for applications developed at their site or applications developed under their governance and that those ADRPs are tested in accordance with the application's designated criticality.
- c. Identifying and training key technical personnel to provide support in the testing of BCP plans for their facility and ADRPs for applications developed at their site, applications developed under their governance, and applications housed at their site or alternate site facilities.
- d. Identifying and training alternate technical personnel to support critical and business-controlled criticality applications in case of disaster.

21 Program Manager, Secure Infrastructure Services

The program manager, Secure Infrastructure Services (SIS), is responsible for the following:

- a. Defining the hardening standards for Postal Service information resources.
- b. Configuring and managing the implementation of personal firewalls on laptops and desktop workstations.
- c. Removing network connectivity from any computing device that does not meet the defined operating system and anti-virus software and recognition pattern thresholds.
- d. Providing consulting support regarding physical, administrative, and technical security controls and processes that safeguard the availability and integrity of the Postal Service intranet and support the confidentiality of information.
- e. Providing consulting support regarding secure connectivity to the Postal Service intranet.
- f. Providing consulting support regarding network services and protocols used by Postal Service information resources.
- g. Implementing and maintaining a secure Postal Service computing infrastructure by setting standards and developing the security processes and procedures.
- h. Implementing and maintaining operational information security throughout the infrastructure.
- i. Coordinating and approving standard configurations for devices.
- j. Recommending and deploying network hardware and software based on the Postal Service security architecture.
- k. Approving network services and protocols.
- l. Monitoring and tracking all physical connections between any component of the Postal Service telecommunications infrastructure and any other information resource not under Postal Service control.
- m. Ensuring secure and appropriate management of the Postal Service Managed Network Services (MNS).
- n. Implementing security controls and processes that will safeguard the availability and integrity of the MNS.
- o. Determining the standards and configuration for secure enclaves.
- p. Assessing information resources to determine the need for placement in a secure enclave.
- q. Ensuring that network services and protocols used by Postal Service information resources provide the appropriate level of security for the MNS.
- r. Implementing secure methods of remote access and appropriate remote access controls.

- s. Implementing secure identification and authentication mechanisms including strong authentication, digital certificates, digital signatures, biometrics, smart cards, tokens, and the associated infrastructure.
- t. Ensuring that only Postal Service–approved encryption products are used.
- u. Implementing appropriate security administration and managing accounts appropriately.
- v. Maintaining the integrity of data and information resources.
- w. Providing security incident detection through perimeter virus scanning and intrusion detection services.
- x. Approving, managing, and ensuring appropriate perimeter virus scanning, penetration testing, and network vulnerability scans and testing.
- y. Ensuring network perimeter security by implementing, approving, and managing firewalls, secure enclaves, proxy servers, intrusion detection services, and intrusion prevention services.
- z. Managing the CIRT to assist the Postal Service to contain, eradicate, document, recover following a computer security incident, and return to a normal operating state.
- aa. Implementing necessary corrective measures learned from incidents or from other sources.
- ab. Ensuring compliance with Postal Service computing infrastructure security standards, processes, and procedures.
- ac. Approving the use of networking monitoring tools, except those used by the OIG.
- ad. Providing support to the OIG during the conduct of investigative activities concerning information security, the computing infrastructures, and network intrusion as requested.
- ae. Monitoring all logs.
- af. Providing network intrusion detection services (IDS).
- ag. Providing network vulnerability testing and analysis services.

22 Network Connectivity Review Board

The NCRB is responsible for the following:

- a. Managing the Postal Service network connectivity process through the implementation of the Handbook AS-805-D, *Information Security Network Connectivity Process*.
- b. Developing system connectivity requirements for Postal Service connections to external systems, externally facing applications (e.g., FTP servers), and connections via the Internet to Postal Service development, production, and internal networks.

- c. Developing standard connectivity and documentation criteria to expedite approval of connectivity requests without additional board action.
- d. Requesting additional information, security reviews, or audits regarding proposed or approved connections, if deemed necessary.
- e. 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.
- f. Consulting with executive sponsors on network information security requirements.
- g. Assisting the requester in identifying alternative solutions for denied requests that are acceptable to the requester and the Postal Service.
- h. Reviewing new information resource, infrastructure, and network connections and their effects on overall Postal Service operations and information security.
- i. Approving network services and protocols.
- j. Recommending changes to the business partner (BP) network. In situations where high risk factors exist, issuing mitigating requirements for connectivity.
- k. 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.

23 Computer Incident Response Team

The CIRT is responsible for the following:

- a. Providing timely and effective response to computer security incidents as they occur.
- b. Working with an organization to contain, eradicate, document, and recover following a computer security incident.
- c. Engaging other Postal Service organizations including, but not limited to, the OIG and Inspection Service.
- d. Escalating information security issues to executive management as required.
- e. Conducting a post-incident analysis, where appropriate, and recommending preventive actions.
- f. Maintaining a system for tracking incidents until they are closed.
- g. Maintaining a repository for documenting and analyzing Postal Service-wide security incidents.
- h. Interfacing with other governmental agencies and private sector computer incident response centers.
- i. Participating in and providing information for Postal Service security awareness.

- j. Developing and documenting processes for incident reporting and management.
- k. Providing support to the OIG and the Inspection Service, as requested.

24 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.

25 Contracting Officers and Contracting Officer Representatives

Contracting officers and contracting officer representatives 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.

26 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 are in place that allow monitoring and auditing of any information resource project.

27 Business Partners

Business partners may request connectivity to Postal Service network facilities for legitimate business needs. Business partners requesting or utilizing 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 and recover from it.
- g. Documenting all conversations and actions regarding the security incident.
- h. Allowing site security reviews by the Postal Inspection Service and CISO.
- i. Allowing audits by the OIG.

28 Project Managers

Project managers for the information resource development, acquisition, or integration project are responsible for the following:

- a. Managing day-to-day development and implementation efforts for new information resources.
- b. Incorporating the appropriate security controls in all information resources.
- c. Updating the EIR on behalf of the portfolio manager.

29 Accreditor

The manager, Corporate Information Security Office, functions as the accreditor and is responsible for the following:

- a. Reviewing the risk mitigation plan and supporting ISA 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 application 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 ISA documentation package to the portfolio manager and executive sponsor.

30 Certifier

The manager, Information Security Assurance, who is appointed by the CISO, functions as the certifier and is responsible for the following:

- a. Managing and providing guidance to the information systems security officers (ISSOs).
- b. Reviewing the ISA evaluation report and the supporting ISA documentation package.
- c. Escalating security concerns or preparing and signing a certification letter.
- d. Forwarding the certification letter and ISA documentation package to the portfolio manager.
- e. Maintaining an inventory of all information resources that have completed the ISA process.

31 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 ASM 271.3). 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 sensitive, critical, or business-controlled information resources.
- 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 ensuring the completion of a PS Form 1360, *Information Security Incident Report*, or acceptable facsimile.
- i. Providing support to the CIRT for incident containment and response, as requested.
- j. Responding to physical security incidents.
- k. Reporting physical security incidents to the Inspection Service.
- l. Interfacing with CIRT, Inspection Service, CISO, or OIG-CIU, as required.

32 Information Systems Security Officers

ISSOs are responsible for the following:

- a. Chairing the ISA team.
- b. Coordinating the completion of the BIA and ensuring that the sensitivity and criticality designations and RTO are properly recorded in the EIR.
- c. Providing advice and consulting support to executive sponsors regarding the security requirements and controls necessary to protect information resources, based on the resources' sensitivity and criticality designation.
- d. Providing guidance on potential threats and vulnerabilities to information resources, appropriate choice of countermeasures, and the ISA process.
- e. Conducting site security reviews or assisting the Inspection Service in conducting them.
- f. Reviewing the ISA documentation package.
- g. Preparing the evaluation report.

33 Information Systems Security Officers

Information systems security officers (ISSOs) are responsible for the following:

- a. Chairing the ISA team.
- b. Ensuring that a risk analysis and business impact assessment (BIA) are completed for each application system.

- c. Ensuring that a risk analysis and infrastructure impact assessment (IIA) are completed for each infrastructure component.
- d. Ensuring that the responsible program manager records the sensitivity and criticality designations in the Enterprise Information Repository (EIR).
- e. Advising and consulting with executive sponsors and portfolio managers during the BIA and IIA processes so they know about (1) security requirements for information resources and (2) mandatory security requirements for information resources when the resources are designated sensitive or critical.
- f. Specifying additional mandatory security requirements based on federal legislation (e.g., HIPAA), federal regulation (e.g., requirements for cryptographic modules), federal directive (e.g., personal identity verification), industry requirement (e.g., payment card industry), the operating environment (e.g., hosted in the DMZ), and the risks associated with the information resource.
- g. Recommending discretionary security requirements to executive sponsors and portfolio managers during the BIA and IIA processes, based on generally accepted industry practices.
- h. Providing guidance on how information resources are vulnerable to threats, what countermeasures are appropriate, and the ISA process.
- i. Conducting site security reviews or helping the Inspection Service conduct them.
- j. Reviewing the ISA documentation package.
- k. Preparing the ISA evaluation report.

34 System Administrators

System administrators are technical personnel who serve as computer systems, network, firewall, and database 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 guidelines 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 updated and 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 information.
- 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 and assisting in the containment of security incidents as required.
- s. Taking action as directed by the CIRT and initiating a PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.
- t. Participating in follow-up calls with the CIRT.
- u. Fixing issues identified following an incident.
- v. Ensuring that virus protection software and signature files are updated and kept current for resources under their control.
- w. Ensuring the availability of information resources by implementing backup and recovery procedures.
- x. Ensuring the compliance with Postal Service information security policy and procedures.

- y. Monitoring the implementation of network security mechanisms to ensure that they are functioning properly and are in compliance with established security policies.
- z. Assisting with periodic reviews, audits, troubleshooting, and investigations, as requested.
- aa. Maintaining a record of all monitoring activities for information resources under their control.

35 Database Administrators

Database administrators (DBAs) are responsible for the following:

- a. Implementing appropriate database security based on the platform-specific hardening guidelines 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 information.
- 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 applications to ensure that security mechanisms are functioning properly.
- l. Tracking hardware and 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 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. Taking action as directed by the CIRT and initiating a PS 1360 as required.

36 All Personnel

All personnel, including employees, consultants, subcontractors, business partners, customers who access non-publicly available Postal Service information resources (such as 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 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. 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 (VPNs), modem

access, dial-in access, secure telecommuting, and remote management and maintenance.

- n. Complying with acceptable use policies.
- o. Maintaining an accurate inventory of databases 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.
- u. Completing PS Form 1360, *Information Security Incident Report*, or an acceptable facsimile.

This page intentionally left blank

Appendix B

Related Information Security Documents

Administrative Support Manual (ASM)

Subchapter 27, *Security*

Subchapter 28, *Emergency Preparedness*

Chapter 8, *Information Resources*

Handbooks

AS-805-C, *Information Security for General Users*

AS-816, *Open VMS Security*

AS-353, *Guide to Privacy and the Freedom of Information Act*

Management Instructions

AS-841-2004-11, *Integrated Solutions Methodology/System Development Life Cycle*

AS-850-2002-10, *Information Technology Change and Configuration Management*

AS-860-2003-2, *Data Stewardship: Data Sharing Roles and Responsibilities*

AS-870-2005-2, *Electronic Messaging (e-mail)*

EL-660-2004-3, *Limited Personal Use of Government Office Equipment Including Information Technology*

Other Related Documents

Enterprise Information Security Architecture

USPS Public Key Infrastructure (PKI) X.509 Certificate Policy (CP)

USPS Root Certificate Authority (CA) Certificate Practice Statement (CPS)

USPS Intermediate Certificate Authority (CA) Certificate Practice Statement (CPS)

USPS Subordinate Certificate Authority (CA) Certificate Practice Statement (CPS)

Boilerplate for Contracts and Agreements

Other Related Documents (*continued*)

Guidelines for New Development of Web-based Applications

Guide to Coding Secure Software

Information Security Code Review Standards

COTS Software Security Evaluation Process

Pub 805-A, *Information Security Assurance (ISA)*

Pub 805-B, *Information Security (bookmark)*

Pub 805-E, *What Every Employee Needs to Know About Information Security*

PS Form 1357, *Request for Computer Access*

PS Form 1360, *Information Security Incident Report*