

For: FSA Employees and Contractors

FSA Information Security Program Policy (ISPP) Update

Approved by: Associate Administrator for Operations and Management



1 Amendments to ISPP

A Background

The current ISPP is on the Information Security Office (ISO) web site at <https://fsa.sc.egov.usda.gov/mgr/iso/public>. The ISO web site is the repository for FSA security policies and guidance.

The ISPP link to the FSA security policies and guidance is also located on the FSA Intranet Handbooks site at <http://fsaintranet.sc.egov.usda.gov/dam/handbooks/handbooks.asp>.

B Purpose

This notice announces amendments to ISPP. The ISO web site security policy repository is updated to reflect the amendments. See Exhibit 1.

C Contacts

Direct any questions about this notice to either of the following:

- Brian Davies, FSA, Information Systems Security Program Manager (ISSPM), by either of the following:
 - e-mail to brian.davies@usda.gov
 - telephone at 202-720-2419
- Michael Serrone, Chief Information Security Officer, by either of the following:
 - e-mail to michael.serrone@usda.gov
 - telephone at 816-926-6567.

Disposal Date	Distribution
March 1, 2012	All FSA employees and contractors; State Offices relay to County Offices

ISPP Amendments

Rules of Behavior – Responsible and Acceptable Use

Section 3, Limited Personal Use (Authorized Personal Use for Non-Government Purposes), subparagraph (iii) Use of Social Networking Sites, has been amended to remove the note: “USDA currently blocks access to some sites, such as Facebook, for security reasons.”

Access Policy

Section 2, Access Control Management, has been amended to include a subparagraph entitled Access Change Requests, which explains required recordation for the Access Change Request Process.

Section 2, subparagraph (c) Account Management, has been amended to include account activation restrictions for newly hired employees and contractors.

Section 2, subparagraph (e) Groups, (ii) has been amended to include the requirement to have group membership documented and approved.

Section 2, subparagraph (f) Identifiers, (iv) has been amended to include the requirement for deleting identifiers or users IDs.

Section 2, subparagraph (g) Reviews, has been amended to include the requirement for authorizing official reviews.

Section 8, External Access, (f) has been amended to prohibit security functions performed through external access.

Personnel Security Policy

Section 4, Basic Security Awareness & Specialized Security Training, has been amended to clarify requirements for new personnel and continued access; and to emphasize the need to obey established target dates for training.

Physical Facility Policy

The General Policy paragraph has been amended to include the types (confidentiality, integrity, and availability) and extent of protection required for information systems.

Section 1, Physical Facilities Security Guidelines, has been removed.

ISPP Amendments (Continued)**Security Planning, Certification, Authorization and Risk Management Policy**

Section 1, Secure Enterprise Architecture:

- (a) has been revised to clarify that all information systems must be tracked in a “centralized” inventory system.
- (c) has been revised to require that unacceptable risks are not created during implementation of an information system.
- (d) has been revised to expect support services to comply with USDA information security requirements and be able to demonstrate compliancy.
- (e) references to change controlled and configuration management during the development phase and tracking security flaws have been removed.
- (f) references to the Rules of Behavior have been removed.

Section 7, Assessments and Risk Management:

- (c) and (d) have been rewritten to emphasize that privacy analysis and assessments must be completed before implementation; risk assessments must be documented in the Department’s enterprise tool; results must be reviewed; and assessments conducted annually or when a significant system change occurs.

Disaster & Contingency Planning Policy

Section 4, Backup & Recovery, has been amended to include minimum (annually) frequency for testing backup media for moderate system.

Configuration Management & Maintenance Policy

The General Policy paragraph has been amended to include the frequency (annually) of policy and procedure development, updates, and dissemination.

Section 2, System Configuration Documentation:

- (a)(i) has been amended to clarify when the baseline system, configuration management process, and system configuration must be reviewed.
- (b) has been amended to require prior review and approval of functional changes by a Configuration Control Change Board.
- (c) has been added to require reviews of all activities associated with controlled changes to the system.

ISPP Amendments (Continued)**Configuration Management & Maintenance Policy (Continued)**

Section 3, System Testing, Review & Approval, (d) and (f) have been amended to clarify when the baseline system, configuration management process, and system configuration must be reviewed.

Section 5, System Maintenance, (a)(iii) has been amended to include “All” IT equipment in the sanitization, maintenance, and disposal process.

System Log Policy

The General Policy paragraph has been amended to include requirements for data extracts from databases holding sensitive information.

Section 2, Storage & Processing Requirements, (c) has been amended to include examples of authoritative time sources.

Removable Media & Portable Device Policy

Section 1, Authorized Use, has been amended to clarify restrictions on storing, processing, or transmitting non-public information; use and types of non-government removable media devices; and unauthorized connections.

Section 1, Authorized Use, has been amended to include mandatory authorization for use of, and the necessity to scan government issued portable device when traveling in and out of the United States; and to include restrictions on wireless connections.

Section 2, Protection from Unauthorized Access, has been amended to identify PII as sensitive information; require encryption of PII during transport; and to expand on the requirements of sanitization mechanisms and physical destruction of media containing no-public information.

Note: In some instances, policy sections and subparagraphs are renumbered to accommodate the amendments.