

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> that is repository for FSA security policies and guidance
- FSA Intranet Handbooks web site at <http://fsaintranet.sc.egov.usda.gov/dam/handbooks/handbooks.asp> that is the location for FSA security policies and guidance.

B Purpose

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

C Contacts

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

- Brian Davies, Information Systems Security Program Manager, 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 January 1, 2014	Distribution All FSA employees and contractors; State Offices relay to County Offices
---	--

ISPP Amendments

Overall

All policy sections referring to mobile devices have been updated to show more relevant examples (e.g., Apple® devices, BlackBerry® smartphones, MP3 players, etc.).

Rules of Behavior

Section 1, Rules of Behavior:

- (g) Official Use of Social Networking Sites (USDA Web 2.0 - New Media), (i) has been amended to include a reference to a new FSA notice (INFO-56) establishing Web Services Office (WSO) to support FSA Web Operations. This notice announces the roles and responsibilities for multiple web tools managed by WSO.

Access Control Policy

Section 3, Password and Authentication:

- (a) Authenticator Management

- (vii) has been amended to add a note that Application gateway accounts are exempt from the 60 day password maximum age limit.

Personnel Security Policy

Section 3, Personnel Security Management:

- (c) Has been amended to state - Upon transfer or re-assignment, and if necessary, the user's Approving Official reviews information systems/facilities access authorizations and initiates appropriate actions (e.g., collecting/reissuing keys, identification cards, building passes; and changing system access authorizations) within 5 business days.
- (d) Has been amended to state - Access agreements (e.g., completed security training/rules of behavior, etc.) must be completed prior to gaining access to information or systems.

Incident Response Policy

Section 1, Incident Reporting:

- (a) Has been amended to state - Upon determination or as quickly as possible, all personnel must report suspected security incidents to the FSA Incident Response Team (FSA-IRT) at 800-255-2434, Option 2 or fsa.incidents@wdc.usda.gov. Also a note was added - Incidents involving PII must be reported within 1 hour of determination.

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

Section 4, System Security Documentation:

- (d) Has been amended to clarify only persistent connections to external information systems must document connection authorization with an Interconnection Security Agreement. Also a note was added - Non-persistent connections (e.g. Connect: direct, secure FTP upload/download) required by law or regulation (i.e. to report tax data) do not require an Interconnection Security Agreement or Data Sharing Agreement.

Section 8, Continuous Monitoring:

- (h) Has been amended to document the timeframe of which information system vulnerabilities must be remediated. 30 days for high risk, 90 days for moderate risk; low risk shall be remediated in accordance with an organizational assessment of risk. Also a note was added - Remediation of vulnerabilities on general support systems not managed by FSA is performed by service providers (e.g., ITS, NFC, NITC, etc.).
- (i) Has been amended to document the timeframe of which information system integrity scans must be ran (quarterly). Also a note was added - Regardless of the FIPS 199 categorization, information systems residing on antiquated platforms (e.g., AS400/S36, Mainframe, etc.) that do not support application level integrity scans are exempt.