

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 polices and guidance.

The ISPP link to the FSA security policies and guidance is also located on the FSA Intranet Handbooks web 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, by either of the following:
  - e-mail to [brian.davies@usda.gov](mailto: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](mailto:michael.serrone@usda.gov)
  - telephone at 816-926-6567.

<b>Disposal Date</b>	<b>Distribution</b>
August 1, 2013	All FSA employees and contractors; State Offices relay to County Offices

## ISPP Amendments

### Rules of Behavior

Section 3, Rules of Behavior, subparagraph (g) Official Use of Social Networking Sites (USDA Web 2.0 - New Media), (i) has been amended to include a reference to a Notice INFO-54 about new media roles and responsibilities. New FSA users supporting these activities, representing USDA, should use an e-mail address or web sites created specifically and solely for official duties that are separate from personal accounts for private use.

Section 6, Protecting Personally Identifiable Information (PII), subparagraph (e) Restrictions on the Transmission or Electronic Transfer of Privacy Act Protected Data, (iii) has been amended to provide that e-mail within the FSA network is protected and encrypted in transit and at rest. The FSA Information Security Office encourages that all PII and sensitive data be encrypted with a second level of protection by using an attachment password protection (Microsoft Word, Adobe PDF, WinZip, etc...). Outlook also has a second level of protection that can be used for transferring PII and sensitive data in the body of the e-mail.

### Access Control Policy

Section 2, Access Account Management, subparagraph (f) identifiers, (iv) has been amended to provide that user accounts may be deleted at 180 consecutive calendar days of inactivity.

Section 3, Password and Authentication, subparagraph (a) Authenticator, (iii) has been amended to provide passwords may only be distributed verbally or by encrypted transmission.

### Contingency Planning Policy

Section 2, System Contingency Planning Activities, subparagraph (d) was added to provide other test or exercise methods may be used.

### System Log Policy

Section 1, Log Record Requirements has been amended to clarify:

- (a) the minimum events that are required to be logged
- (b) only the defined events to be logged (not events themselves) must be reviewed and updated at least annually.

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