UNITED STATES DEPARTMENT OF AGRICULTURE
Farm Service Agency
Washington, DC 20250

Notice IRM-464

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://sharepoint.fsa.usda.net/mgr/iso/public/Wiki%20Pages/Home.aspx**. 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 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, FSA Information Systems Security Program Manager (ISSPM), by either of the following:
  - e-mail to **brian.davies@wdc.usda.gov**
  - telephone at 202-720-2419
- Michael Serrone, FSA Chief Information Security Officer (CISO), by either of the following:
  - e-mail to **michael.serrone@kcc.usda.gov**
  - telephone at 816-926-6567.

Disposal Date	**Distribution**
March 1, 2015	All FSA employees and contractors; State Offices relay to County Offices

ISPP Amendments

Rules of Behavior

B. Policy Detail, (2) Acceptable use, (e) Telework/Flexiplace Rules:

(vii) Has been amended to include the following note: "Personal equipment must be approved for government use (e.g., PC on a stick, etc.). Also, copying any non-personal government-owned data (e.g., source code, PII, sensitive information, etc.) to personal equipment is prohibited.".

Security Planning, Certification, Authorization and Risk Management Policy

B. Policy Detail, (4) System Security Documentation:

(a) Has been amended to include the following note: "For specific guidance on USDA's implementation of reviewing and updating security plans, refer to the most current Risk Management Framework Process Guide issued by USDA.".

Contingency Planning Policy

B. Policy Detail, (3). Alternate Sites (Not Applicable to Low systems):

(a) Has been amended to include examples of alternate sites to the following policy: "System backup information must be stored at an alternate site (e.g., bank, school, FSA employee's home, neighboring county office, etc.) with agreements that support the storage and recovery of backups according to the recovery time objective of the system.".

(a) Has been amended to include the following note: "If backup information is stored in a fireproof safe or file cabinet that has a UL rating of 150, an alternate site is not required.".

Removable Media and Portable Device Policy

A. General Policy has been amended to include the following note: "Non-government factory-sealed removable media (e.g., thumb drive, CD, DVD, etc.) is authorized to be attached to government computing equipment only once.". Although this note speaks to every scenario for attaching removable media to our government computing equipment, it was added to specifically allow a means for FSA customers to obtain their own farming information from our field offices in an electronic format.