

For: FSA Employees

Using FSA-13-A's

Approved by: Associate Administrator for Operations and Management



1 Overview

A Background

FSA has procedures to request adding, modifying, and deleting access privileges to USDA and FSA information technology systems.

B Purpose

This notice:

- explains that FSA-13-A **must** be submitted **each** time a user requests addition or modifications to their current computer access; deletions of user access may be processed using FSA-13-A, AD-1106, AD-1106-1 and/or SF-52
- explains that USDA and FSA **mandatory** Information Security Awareness and Rules of Behavior Training, along with the Special Agreement Check **must** be completed **before** access is granted for new users
- explains the revised processes of requesting new hire access, adding access, modifying access, deleting access, or separated employee access to user accounts for any USDA or FSA application
- replaces all preceding FSA-13-A's and procedures used to request system access, including FSA-13-A (03-06-09)
- includes the following responsibilities and instructions:
 - submission guidance and responsibilities
 - requirements for requesting security access using revised FSA-13-A.

C Contact

For questions about this notice, contact Roger Scaife at 202-720-9152 or Jeff Wagner at 816-926-6747.

Disposal Date	Distribution
October 1, 2010 5-20-10	All FSA Employees; State Offices relay to County Offices

Notice IRM-430

1 Overview (Continued)

D Security Liaison Representative (SLR) Contacts

SLR's are designees who serve as the security liaison to the FSA Information Security Office (ISO) to assist with granting, modifying, and/or removing access. Appropriate SLR's may be contacted as follows:

- State and county employees contact State SLR
- APFO contact Lori Uhlhorn at 801-844-2970
- Washington, DC; Kansas City, MO; and St. Louis, MO; contact the ISO operations team at 800-255-2434, Option 2, and Option 5.

2 Access Request Procedures

A Requesting Access for New Users

Supervisors and contracting officer technical representatives (COTR's) **must** ensure that USDA and FSA **mandatory** Information Security Awareness and Rules of Behavior Training (ISA/RBT), along with the Special Agreement Check (SAC) (that is initial fingerprint results) are completed and approved for every new FSA employee or contractor that needs computer access. ISO will verify with HRD that SAC and ISA/RBT are completed.

If SAC or ISA/RBT is not completed, ISO will not process the request or grant access to any system.

SAC's are supplied by HRD for Federal employees and by the Emergency Preparedness Division (EPD) for contract employees. EPD submits the results to COTR and HRD receives the results for Federal employees.

OMB Memorandum M-07-17, dated May 22, 2007, states that "Agencies must initially train their employees on their privacy and security responsibilities before permitting access to agency information and information systems." Detailed FSA ISA/RBT requirements are in Notice IRM-420.

When requesting computer access privileges for a new hire, the supervisor or COTR **must**:

- determine the access needed by the new user
- for all new hires that completed the paper-based training, attach the FY 2010 ISA/RBT completion certificate to FSA-13-A

Note: Contractors are **required** to complete the web-based training version.

Notice IRM-430

2 Access Request Procedures (Continued)

A Requesting Access for New Users (Continued)

- complete FSA-13-A requesting access to any FSA, International Technology Services (ITS), or other agency systems or applications
- sign and submit all FSA-13-A's to the appropriate SLR.

Note: Certain systems and applications require submitting specialized forms in addition to FSA-13-A. This notice does **not** obsolete, prohibit, or supersede using those forms; including, but **not** limited to AD-1143 for NFC Corporate Systems and AD-2017 for SCIMS.

B Requesting Additional Access, Modified Access, or Deleting Access for Current Users

FSA-13-A **must** be submitted **each** time a user requests additions or modifications to their current computer access. Deletions of user access may be processed using FSA-13-A, AD-1106, AD-1106-1, and/or SF-52.

Note: If the user is leaving FSA, subparagraph C applies rather than this subparagraph.

If user works in 1 office and needs access to web-based applications in another office, the user's supervisor **must** submit FSA-13-A. In FSA-13-A, block 18 enter the user's eAuthentication user ID and the office name where they will be working. When user is no longer working in the other office, submit FSA-13-A to delete that access.

C Requesting Deletion of User Accounts for Separated Employees

When user leaves FSA employment, their computer access **must** be deleted by submitting either of the following:

- the following document, as applicable; for:
 - Washington, DC, AD-1106 and/or FSA-13-A
 - Kansas City, MO; St. Louis, MO; and Salt Lake City, UT, AD-1106-1 and/or FSA-13-A
 - all other offices, FSA-13-A
- SF-52 to ISO operations team by FAX to 816-627-0687 or SLR, as applicable.

In addition to submitted documentation, ISO will use reports to identify users that have left FSA and will take the appropriate actions to ensure that accesses are deleted.

Notice IRM-430

3 SLR and/or Supervisor/COTR and ISO Operations Team Responsibilities

A SLR and/or Supervisor/COTR Responsibilities

SLR and/or supervisor/COTR shall maintain all copies of the following, as applicable, by employee/contractor name:

- AD-1106 and/or FSA-13-A for Washington, DC
- AD-1106-1 and/or FSA-13-A for Kansas City, St. Louis, MO; and Salt Lake City, UT
- FSA-13-A for all other offices
- SF-52.

B ISO Responsibilities

ISO operations team is responsible for the following:

- processing FSA-13-A parts
- submitting FSA-13-A to the appropriate group for additional processing, such as NFC, NITC, ITS, etc.
- maintaining electronic and/or paper copies of FSA-13-A
- contacting SLR's, individuals, and/or supervisors/COTR's when completed
- reviewing a sample of applications quarterly to which users have access privileges
- reviewing active ID's on FSA systems and applications.