

For: FSA Employees and Contract Employees

FSA Computer Security Agreement

Approved by: Deputy Administrator, Management



1 FSA-13's (10-11-07)

A Background

In FY 2006, FSA had an independent audit review (per OMB Circular A-123) that determined that improvements could be made in FSA's security access request processes and procedures. FSA management and the Information Security Office (ISO) implemented the following to improve the access request process:

- review of current procedures and forms used by FSA for collecting, processing, and controlling information security access requests
- improvements to security access request procedures.

B Purpose

This notice:

- requires that **all** FSA users **must** have **new** FSA-13's, dated (10-11-07) on file
- provides guidance and instructions for completing FSA-13's (10-11-07), see Exhibit 1.

Notes: All previous versions of FSA-13 are **obsolete**.

This notice impacts all security access requests for all FSA information system users by employees and contractors.

C Sources of Authority

The sources of authority are 6-IRM, Notices 1-DCP, IRM-388, CM-560, CM-562, Departmental Manuals USDA DM-3500, USDA DR3602-001, OCIO/ITS Security Policy Manual, OMB Circular A-123, and OMB A-130.

Disposal Date	Distribution
January 1, 2008	All FSA Employees and Contract Employees; State Offices relay to County Offices

Notice IRM-401

1 FSA-13's (10-11-07) (Continued)

D Affected Users

All employees and contractors that use or will be using government information technology hardware (such as LAN/Network and Mainframe Access) **must** submit FSA-13 (10-11-07) by **November 30, 2007**, to continue to access FSA computers and applications. FSA-13 (10-11-07) is available from the FFAS Employees Forms Online Website at **<http://intra3.fsa.usda.gov/dam/ffasforms/forms.html>**.

Future requests to modify, add, or delete a user's access to FSA applications **must** have a current FSA-13 (10-11-07) on file for the user with their Security Liaison Representative (SLR) or ISO.

Note: SLR's are required to maintain and validate that FSA-13's (10-11-07) are on file for their offices.

E Access Privileges

For more information on access privileges, contact the ITSD, ISO, Information Security Operations Support (ISOS) staff, by:

- telephone at 1-800-255-2434, Option 2
- e-mail to **security@kcc.usda.gov**
- FAX at **816-627-0687**.

F Handling New FSA-13's

Follow Notice IRM-400 for completing and submitting new FSA-13's to SLR/ISOS.

This table provides personnel responsible for maintaining FSA-13's.

Location	FSA-13 Responsibilities
<ul style="list-style-type: none">• County Office• District Office• State Office	Supervisor/COTR shall submit FSA-13 to the designated SLR. SLR's shall submit and maintain FSA-13's for their Offices.
<ul style="list-style-type: none">• National Office• Kansas City• St. Louis• APFO	Supervisor/COTR shall submit FSA-13's to ISOS. ISOS shall maintain FSA-13's for these offices until SLR's are assigned.

FSA-13 (10-11-07)

The following is the current version of FSA-13 (10-11-07).

Note: All previous versions are obsolete.

<p><small>This form is available electronically. FSA-13 (10-11-07)</small></p>	<p>U.S. DEPARTMENT OF AGRICULTURE Farm Service Agency</p>	
<p>FSA COMPUTER SECURITY AGREEMENT</p>		
<p>An agreement between _____ and the USDA/Farm Service Agency (FSA). (Print or Type Name)</p>		
<p>1. PURPOSE. This document is meant to obtain an individual agreement to abide by security requirements and procedures needed to protect FSA and customer information resources. It is also intended to help raise security awareness and inform workers about security policies and procedures and to provide workers an opportunity for asking questions about these matters.</p>		
<p>2. AUTHORITIES. National policy requirements regarding information systems are stated in the Federal Information Security Management Act (Title III of the E-Government Act of 2002); the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 [1993]); Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control; and OMB Circular A-130, Management of Federal Information Resources. These documents along with USDA security policies prescribe and set standards for establishing and maintaining a comprehensive information security program and use of information systems.</p>		
<p>3. SCOPE. This agreement applies to FSA workers (both employees and contractors) who operate, maintain, and/or use Information Technology (IT) systems.</p>		
<p>4. UNDERSTANDING AND AGREEMENTS. As a user of IT systems, I:</p>		
<ul style="list-style-type: none"> • Will protect FSA and customer systems in accordance with Federal, USDA, FSA and OCIO policies. • Will use USDA and/or FSA computer systems (e.g., computers, systems, laptops, PEDs, networks, etc.) only for authorized purposes. If using the computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy, supervisor approval, and without interfering with official business. • Will protect systems and all sensitive information from electronic or physical access by unauthorized personnel. I will protect computer equipment, media, telecommunications, and similar assets from theft, fraud, misuse, loss, unauthorized modification, and unauthorized denial of use. I will make every effort to avoid action/inaction that could jeopardize mission success, customer rights, individual privacy, or the reputation of the FSA. • Understand that systems and other information resources, including electronic mail and Internet access, are primarily intended for official business and may be monitored. Although FSA policy permits limited personal use, I understand that my personal use must not interfere with official business and that I have no expectation of personal privacy when using these systems. • Will not intentionally access, delete or alter files, operating systems or programs, except as specifically authorized for official business. • Will not leave FSA computers in an operational state (e.g., "logged on") while unattended. I will either turn off the computer system, manually lock the screen, or set a time activated password-protected screen saver. • Will abide by software copyright licenses and restrictions. I will not load any unapproved software (e.g., software from home, games, etc.) or install hardware or peripheral devices (e.g., external hard drives, docking stations, thumb drives, etc) on FSA systems without my supervisor's permission. • Will not download file-sharing software (e.g., MP3 music, video files, etc.), peer-to-peer software (e.g., Kazaa, Napster, etc.), or games onto FSA systems or networks. 		
<p>_____ (User Initials)</p>		

FSA-13 (10-11-07) (Continued)

FSA-13 (10-11-07)

Page 2 of 3

- Acknowledge that I will receive user identifiers (user IDs) and passwords to authenticate my computer account. After receiving them, I will:
 - Immediately change the password.
 - Protect and not share or publicly post my password. If my password has been compromised, I will report the issue to my supervisor or security personnel.
 - Not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED) or other media unless approved by security personnel.
 - Be responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when logged on a system with that account.
 - Ensure my password is changed regularly or if compromised.
 - Ensure my password meets USDA complexity requirements.
- Will use anti-virus software in an effective way to prevent damage or disruption to FSA operations. I will scan all removable media (e.g., disks, CDs, thumb drives, etc.) for malicious software (e.g., viruses, worms, etc.) before using it on any government owned computer system or network.
- Will take appropriate steps to protect important data from loss (e.g., backups).
- Will not use Government owned computers, networks or IT services for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, and so forth. If I use Government owned computer systems and networks, I will do so within the bounds allowed by USDA policy and supervisor approval and without interfering with official business.
- Will not try to disable or subvert ITS and FSA security controls or monitoring mechanisms.
- Will not attempt to break into any computer, whether Federal, USDA, or private, for which access is not authorized. Attempted break-ins may be authorized by my organization's Information System Security Program Manager (ISSPM) only for functions such as approved security tests, approved attempts to recover a system after a password is lost/forgotten, and similar functions.
- Will practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.
- Will report suspected/actual security incidents and other security concerns to my supervisor and my organization's ISSPM.
- Will stay abreast of security issues through education and awareness products distributed throughout USDA. I will attend at least one (1) security awareness session each year.
- Will not disclose sensitive data. In the course of performing work at FSA, I realize it may be necessary for me to have access to sensitive information, which includes:
 - Proprietary information – technical information or trade secrets, that is proprietary.
 - Privacy information – information protected under the provisions of the Privacy Act of 1974.
 - Privileged information – financial or commercial information that must be restricted from disclosure on the basis of Federal law or contractual agreement.
 - Government information – information or data stored, processed or handled in providing services under any FSA contract.

 (User Initials)

FSA-13 (10-11-07) (Continued)

FSA-13 (10-11-07)

Page 3 of 3

I have read and understand the FSA Security Agreement on the use of government Information Technology (IT) systems. I understand that unauthorized or inappropriate use of government IT systems may result in the loss or limitation of my privilege. I also understand that I could face administrative action ranging from counseling to removal from the agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

5. EFFECTIVE DATE. This agreement becomes effective when signed and dated. Refusal to sign may result in being denied use of any or all USDA information systems including e-mail and network access to the Internet.

NOTE: Refusal to sign does not relieve the individual of responsibility to abide by the standards set forth in this and related documents. (Supervisor/COR/COTR: If the worker refuses to sign, notate that fact on the signature line and retain this document.)

6. User's Signature		7. Telephone Number	8. Date
9. Employee Type (Check applicable box): <input type="checkbox"/> KC <input type="checkbox"/> STL <input type="checkbox"/> WDC <input type="checkbox"/> ST/CO <input type="checkbox"/> CONTRACTOR <input type="checkbox"/> OTHER (Specify):			
10. Organization		11. If Contractor – Company Employed By	
12. Supervisor/COR/COTR Signature		13. Supervisor/COR/COTR Title	14. Date

USDA IS AN EQUAL OPPORTUNITY EMPLOYER