

For: FSA Offices

FY 2010 Mandatory Role-Based Information Technology (IT) Security Training

Approved by: Deputy Administrator, Management



1 Overview

A Background

The Federal Information Security Management Act (FISMA) and OPM have mandated that better attention be devoted to role-based IT security training. Agencies are required to identify and provide role-based IT security training to individuals who have significant responsibilities for information security. Role-based training is the addition or reinforcement of specialized knowledge and skills to facilitate better job performance.

All Federal employees and contractors with significant information security responsibilities or significant impact on IT systems shall complete role-based IT security training annually. Personnel specifically identified in this notice by ITSD as having significant security responsibilities are required to complete the FY 2010 Role-Based IT Security Training using AgLearn and as directed in this notice by **December 20, 2009**.

B Purpose

This notice:

- directs supervisors to identify and ensure that appropriate employees complete role-based IT security training annually
- identifies employees mandated by ITSD to complete role-based IT security training by **December 20, 2009**
- explains procedures for completing the FY 2010 Role-Based IT Security Training using AgLearn.

Disposal Date	Distribution
November 1, 2010	All FSA Offices; State Offices relay to County Offices

Notice IRM-423

1 Overview (Continued)

C Authorities

The following are authorities related to this notice:

- E-Government Act of 2002, Pub. L. 107-347, 44 U.S.C. 3531 et seq., Title III, Federal Information Security Management Act
- 5 CFR Part 930, Employees Responsible for the Management or Use of Federal Computer Systems
- DR 3140-1, Management ADP Security Management
- DM 3545-1, Computer Security and Training, Chapter 9, Part I
- OPM Information Security Awareness and Training Policy promulgated in June 2005.

2 Role-Based IT Security Training Guidance

A Users Mandated to Complete Role-Based IT Security Training

ITSD has identified the following Federal and contractor employees as having significant security responsibilities or a significant impact on management, operational or technical IT security controls. All identified personnel **must** complete at least 1 course listed in the FY 2010 Role-Based IT Security Training Curriculum in AgLearn by **December 20, 2009**:

- Security Liaison Representatives (SLR's) and alternate SLR's, both field and large office
- AgLearn Administrators and alternate AgLearn Administrators
- ITSD staff and contractor employees.

Note: Newly assigned ITSD employees, SLR's, and AgLearn Administrator's shall complete role-based IT security training **before** starting their security related duties.

B Other Employee Selections

Supervisors shall identify any other Federal and contractor employees that may have information security responsibilities or a significant impact on IT systems and provide appropriate role-based IT security training for those employees. Role-based IT security training shall focus on job functions or roles and responsibilities, **not** job title.

Notice IRM

2 Role-Based IT Security Training Guidance (Continued)

B Other Employee Selections (Continued)

Employees from all employment categories shall be considered for role-based IT security training, including but **not** limited to the following:

- Agency Leaders
- Facility Managers
- IT Support Personnel
- Operations Managers
- IT Security Personnel
- Human Resource Representatives
- Webpage Developers
- End Users
- System Managers, Owners, and Administrators.

Use the contact information in subparagraph E to request addition of the role-based IT security training course curriculum to an employee's AgLearn learning plan. Any other assigned role-based IT security training should be used to broaden the employee's knowledge and skills and to help improve performance of their **specialized security** role. Record all training completions in AgLearn according to current training regulations.

C Training Guidance for Mandated Users

All identified personnel are accountable for completing at least 1 of the 11 course options listed under the FY 2010 Role-Based IT Security Training Curriculum in Exhibit 1.

The AgLearn version of the course curriculum **must** be assigned to employees by an AgLearn Administrator and will be accessible in the employee's AgLearn "Curriculum Status".

HRD, Training and Development Branch, National Coordinator for AgLearn Administrators will assign the training curriculum to agency AgLearn Administrators and their alternates.

Notice IRM-423

2 Role-Based IT Security Training Guidance (Continued)

D Accessing the Role-Based Training in AgLearn

Employees shall complete the training according to the steps in the following table. Do not repeat the same course previously completed in FY 2009. Credit will not be given for repeated courses.

Note: Newly appointed SLR's must complete the “**Introduction to ISSP Management**” course.

Step	Action
Start Here ▶	Review Exhibit 1 and select a course most appropriate for individual specialized security role.
1	Access the AgLearn Home Page located at http://www.aglearn.usda.gov .
2	CLICK “ Learner Login ”.
3	On the eAuthentication Login Warning Screen, CLICK “ I Agree ”. Enter user ID and password and CLICK “ Login ”.
4	CLICK “ Learning ”.
5	CLICK “ Curriculum Status ”.
	
6	CLICK “ FSA FY 2010 Role-Based IT Security Training ”.
7	CLICK “▶” next to Curriculum Requirements; this may already be open for some users.
	
8	CLICK “▶” next to 1 item from the item pool. Note: Some course(s) may show a completion date from previous years. Only courses with a completion date for this FY will be accepted for credit.
9	Locate the course the user wants to complete and CLICK “ Launch Content ” to begin or “ Add to Learning Plan ” to complete later. There are 11 courses from which to choose.
10	Ensure that courses show as complete in the learning history. Note: If user completes course number 4, Managing High Risk Situations, Exhibit 1, user will also need to complete the course entitled Operational Risk Models to receive full credit.

Notice IRM-423

2 Role-Based IT Security Training Guidance (Continued)

E Contacts

The following table provides a summary of contacts if there are questions.

IF there is a question about...	THEN...
AgLearn	do any of the following: <ul style="list-style-type: none"> • in AgLearn, CLICK “Help” • in AgLearn, CLICK “Contact Us” • call 1-866-633-9394.
new eAuthentication accounts or password resets	contact ITSD National Help Desk at 1-800-255-2434, option 3, or self-register for an account at http://www.eauth.egov.usda.gov/eauthCreateAccount.html .
this notice or Security Awareness Training policy	contact either of the following: <ul style="list-style-type: none"> • Seabelle Ball by: <ul style="list-style-type: none"> • e-mail at AgLearnSecurity@wdc.usda.gov • telephone at 202-205-7399 • Brian Davies by: <ul style="list-style-type: none"> • e-mail at brian.davies@wdc.usda.gov • telephone at 202-720-2419.
National Office employee training administration	contact Bessy Plaza, HRD, National Office Training by: <ul style="list-style-type: none"> • e-mail at bessy.plaza@wdc.usda.gov • telephone at 202-401-0365.
Kansas City, St. Louis, or APFO employee training administration	contact either of the following: <ul style="list-style-type: none"> • Mark Nelson by: <ul style="list-style-type: none"> • e-mail at mark.nelson@kcc.usda.gov • telephone at 816-926-3420 • Cindy Witmer by: <ul style="list-style-type: none"> • e-mail at cindy.witmer@kcc.usda.gov • telephone at 816-926-2500.
State and County Office employee training administration	contact State training officer or AgLearn lead.

2 Role-Based IT Security Training Guidance (Continued)

F Reasonable Accommodations

Persons who require special accommodations to participate in this training should contact their supervisor or local help desk.

G Noncompliance

Employees that do not comply with the role-based IT security training mandate risk computer account suspension.

H Continuing Security Training Requirements

To facilitate strengthening of the Agency's overall IT Security Training Program and expand on the required annual IT Security Awareness, Rules of Behavior, and Role-Based IT Security Training, offices shall:

- employ subsequent methods, (office posters, booklets, newsletters, handouts, checklists, videos, brown bag lunch series, etc.), to make personnel aware of information security and changes in the security environment of the individual office
- provide additional or refresher training when personnel enters a new position which deals with sensitive information or has different information security requirements.

Note: The additional training should be on the level of responsibility and the sensitivity of the information the employee handles.

Use the National Institute of Standards and Technology (NIST) Special Publications 800-16, Information Technology Security Training Requirements (A Role-and Performance-Based Model) and 800-50, Building an Information Technology Security Awareness and Training Program to help:

- plan
- implement
- maintain
- periodically evaluate ongoing IT security training plans and actions.

NIST Special Publications are located on the NIST web site located at, <http://csrc.nist.gov/publications/PubsSPs.html>.

FY 2010 Role-Based IT Security Training Curriculum

FY2010 Role-Based IT Security Training Curriculum			
Course Name	Course Description	Target Audience	Duration
Introduction to ISSP Management	Introduction to ISSP Management.	New SLR's and AgLearn Administrators.	60 minutes
Information Security for Executives and Managers (Briefing USDA-OCIO-EXECSUMM-PII-V1)	This training will provide an overview of the key information security practices to consider as organization leaders within USDA.	Executive and management, but all employees could benefit.	40 minutes
Malicious Code and Information Security	How malicious code works and the ways to defeat it in a wired and wireless environment. An introduction to information security best practices.	Business users.	100 minutes
<p>A Managing High Risk Situations (30 minutes)</p> <p style="text-align: center;">and</p> <p>B Operational Risk Models (10 minutes)</p>	<p>Presents 9 scenarios in which employees face volatile and potentially violent situations in the workplace and gives participants an opportunity to discuss appropriate resolutions.</p> <p>Involves understanding the negative events associated with people, processing technology, and external events.</p>	GS-15 and Schedule C (all managers and supervisors can benefit).	<p>Total 40 minutes for both courses.</p> <p>Both courses must be completed to get credit</p>
E-mail Etiquette Series	The 12 Immutable Laws of E-mail Etiquette.	All users.	45 minutes
**Privacy and Information Security	<p>The protection of an individual's personal information has business implications that extend beyond the privacy of any 1 individual. Various laws protect private information relative to certain businesses and industries.</p> <p>Example: The Health Insurance Portability and Accountability Act (HIPAA) laws protect private medical information.</p>	All employees, especially those who have access to private information.	60 minutes

FY 2010 Role-Based IT Security Training Curriculum (Continued)

FY2010 Role-Based IT Security Training Curriculum			
Course Name	Course Description	Target Audience	Duration
Security, Safety, and Communication	To understand the role of security in an organization, (data, physical, incident reporting, etc.). The importance of following safety and environmental guidelines, and how to communicate with customers in a professional manner.	Entry level computer technicians and security personnel.	125 minutes
Physical (Environmental) Security	To understand the considerations and mechanisms involved in implementing the physical security of an enterprise.	Mid-level and senior-level managers.	120 minutes
Security and the Wireless Environment	Describes security in the wireless environment.	Technical and security professionals; IT and business managers.	120 minutes
Securing Storage	Recognize the importance of storage security and identify the: <ul style="list-style-type: none"> • tasks involved in ensuring storage security • threats to storage security and how they are mitigated. 	IT professionals with little or no knowledge of storage concepts but who needs to support storage products now or in the future and make storage related decisions.	140 minutes
Workplace Security Awareness	Provides an awareness-level orientation of basic workplace security fundamentals and appropriate actions for workers to complete in the event of potential threat situations that may be encountered in the workplace, including encountering trespassers, receiving phone threats, dealing with workplace violence incidents, evacuating during an emergency, and protecting against various types of terrorist acts.	All new employees (especially those new to security).	60 minutes

Note: ** Recommended for AgLearn Administrators.