

For: FSA Offices

Mandatory Specialized Role-Based Information Technology (IT) Security Training for FY 2012

Approved by: Associate Administrator for Operations and Management



1 Overview

A Background

The Federal Information Security Management Act mandates that employees, contractors, and partners holding positions with significant responsibilities for information security complete specialized role-based IT security training:

- **before** access is granted to any Agency information systems and/or sensitive data
- annually for continued access.

This year’s training course is titled, “**Protecting Personally Identifiable Information**”, with course ID, “**USDA PII**”. It is available on AgLearn and **must** be completed by all **security office and security liaison personnel by March 30, 2012**.

The course will cover what Privacy Act data is and the importance of protecting PII, organizational responsibilities for safeguarding PII, transporting PII, and an individual’s responsibilities for recognizing and safeguarding protected and sensitive data.

Note: The lesson on reporting PII incidents may direct readers to USDA PII contacts. Employees are reminded that specific FSA contacts and instructions for reporting PII incidents can be found on the Information Security Office (ISO), ISO Online web site at <https://fsa.sc.egov.usda.gov/mgr/iso/public/Wiki%20Pages/Incident%20Reporting.aspx>.

B Purpose

This notice provides information about the required specialized role-based IT security training for FY-2012.

Disposal Date August 1, 2012	Distribution All FSA Offices; State Offices relay to County Offices
--	---

2 Training Guidance

A Security Office and Security Liaison Personnel

The Chief ISO (CISO) requires this as **mandatory training** for the following personnel with significant responsibilities for information security. The course has already been added to AgLearn To-Do Lists for the following employees:

- database administrators
- ISO personnel
- MIDAS security support personnel
- State Office security liaison representatives and their backups.

Follow the procedures in paragraph 3 to access To-Do Lists.

B Other Personnel

Supervisors are **required** to train any other personnel with functional responsibilities that may have a significant impact on information security. Employees that should be considered for role-based IT security training include, but are **not** limited to the following:

- end users, system managers, owners, and administrators
- facility managers
- FSA leaders
- human resource representatives
- IT support personnel
- operations managers
- webpage developers.

Follow the procedures in paragraph 3 to add the course to the To-Do List.

C Significant Responsibility for Information Security

USDA, OCIO defines positions that may impact the mission of the Agency through a loss of confidentiality, integrity, and/or availability of the USDA information, regardless of media, are to be designated as having significant responsibilities for security. Some of the determining factors are users requiring advanced rights to a system beyond that of a regular user that may include the following:

- database, network, mail, and IT system administrators
- programmers and security managers
- IT system owners, information owners, and IT system program managers
- CIO's, privacy officers, and FOIA officers
- positions that have programmatic and/or management control over IT system resources.

Note: Users who have administrative access to their own desktops and/or laptops are **not** considered to have significant responsibilities for security.

Notice IRM-449

2 Training Guidance (Continued)

D Training Deadline

The training announced in this notice shall be completed by:

- **March 30, 2012**, for security office and security liaison personnel identified by CISO
- **April 13, 2012**, for all other applicable employees.

3 Accessing the Training

A Accessing Already Assigned PII Training Course for Security Liaison Personnel

Employees identified by CISO will find the course on their AgLearn To-Do List. Access user’s AgLearn To-Do List, launch, and complete the training according to the following table.

Step	Action
1	Access the AgLearn Home Page at http://www.aglearn.usda.gov .
2	CLICK “Login”.
3	On the eAuthentication Login Warning Screen, CLICK “I Agree”. Enter user ID and password and CLICK “Login”.
4	On the AgLearn Home Page, user’s “To-Do List” will be displayed. Place the cursor on the course titled, “Protecting Personally Identifiable Information” and a popup box will be displayed. CLICK “Launch content”.
5	Employees shall complete the course and then check their “Completed Work” in AgLearn to ensure that the training has been marked complete.

Note: Contact bessy.plaza@wdc.usda.gov if the course was not assigned.

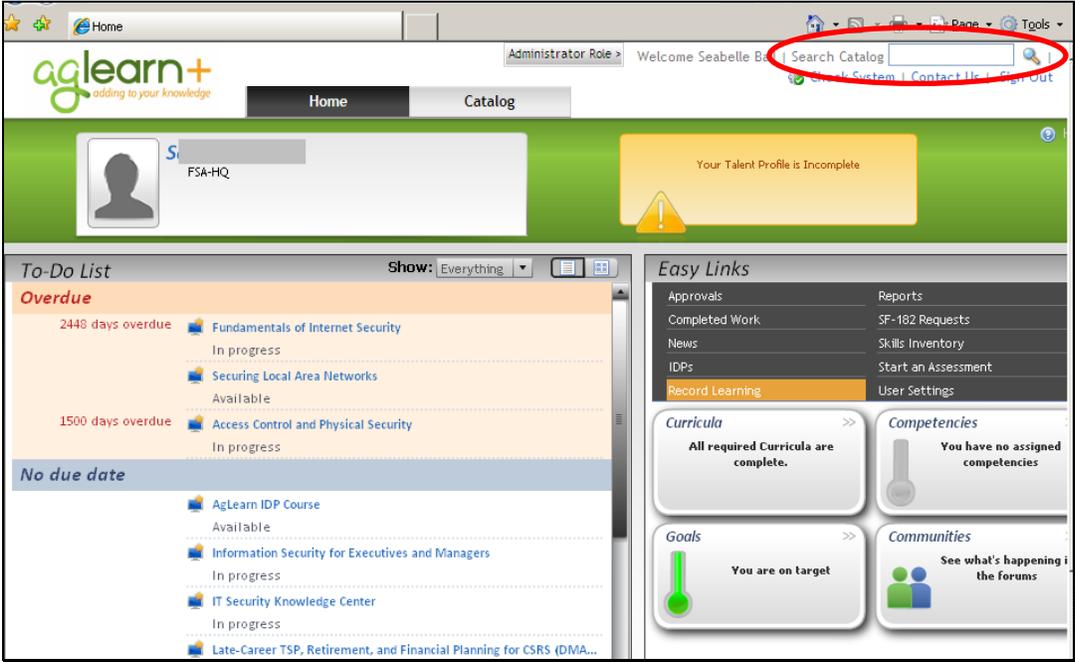
B Locating Unassigned PII Training for Other Personnel

Step	Action
1	Access the AgLearn Home Page at http://www.aglearn.usda.gov .
2	CLICK “Login”.
3	On the eAuthentication Login Warning Screen, CLICK “I Agree”. Enter user ID and password and CLICK “Login”.

Notice IRM-449

3 Accessing the Training (Continued)

B Locating Unassigned PII Training for Other Personnel (Continued)

Step	Action
4	<p>In the “Search Catalog” box at the top of the AgLearn Home Page, enter the course name, “Protecting Personally Identifiable Information” or course ID, “USDA PII”.</p> <p>CLICK “” (the “Go” symbol) and wait for the search results to return the course.</p>  <p>The screenshot shows the AgLearn Home Page. At the top right, there is a search bar labeled "Search Catalog" with a magnifying glass icon to its right. This search bar and icon are circled in red. Below the search bar, there is a navigation menu with "Home" and "Catalog" options. The main content area shows a user profile for "FSA-HQ" and a notification that the "Talent Profile is Incomplete". There are also sections for "To-Do List" and "Easy Links".</p>
5	<p>Locate the returned course and CLICK either of the following:</p> <ul style="list-style-type: none"> • “Add to To-Do List”, users must return to their To-Do List, CLICK “Launch content”, and the course will begin • “Launch content”, the course will begin immediately.
6	<p>Employees shall complete the course and then check their “Completed Work” in AgLearn to ensure that the training has been marked “Complete”.</p>

Note: Contact local training officer or AgLearn lead if help is needed locating and adding a course to the To-Do List.

Notice IRM-449

4 General Information

A Contacts

The following is 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 ITS 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 either of the following: <ul style="list-style-type: none"> • e-mail to seabelle.ball@wdc.usda.gov • telephone at 202-205-7399 • Brian Davies by either of the following: <ul style="list-style-type: none"> • e-mail to brian.davies@wdc.usda.gov • telephone at 202-720-2419.
National Office employee training administration	contact Bessy Plaza, HRD, by either of the following: <ul style="list-style-type: none"> • e-mail to 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 either of the following: <ul style="list-style-type: none"> • e-mail to mark.nelson@kcc.usda.gov • telephone at 816-926-3420 • Cindy Witmer by either of the following: <ul style="list-style-type: none"> • e-mail to cindy.witmer@kcc.usda.gov • telephone at 816-926-2500.
State and County Office employee training administration	contact the State training officer or AgLearn lead.

4 General Information (Continued)

B Reasonable Accommodations

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

C Noncompliance

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

D Continuing Security Training Requirements

To facilitate strengthening FSA's overall IT Security Training Program, FSA 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 that 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, and periodically evaluate ongoing IT security training plans and actions. NIST special publications are located on the NIST web site at <http://csrc.nist.gov/publications/PubsSPs.html>.