LMS Accounts for Training Coordinators, Training Records Managers and Help Desk Staff

Important Instructions: In order to obtain an LMS (learnDOJ) administrator account, all of the following steps must be completed:

1. You must have an active LearnATF user account.

2. You must complete the mandatory "Information Security Awareness" and "Social Engineering" online courses through your LearnATF user account. *Help Desk staff must also complete one of the mandatory role-based IT security online courses. This will be assigned directly to your learning plan after we receive your e-request.*

3. You must submit an e-request for LMS access for the appropriate role (Training Coordinator, Training Records Manager or Help Desk).

4. You must read the "Rules of Behavior" section of this document and fax a signed copy of the Certification Statement on page four to 202-648-9718.

Once your account has been approved, you will be sent an email from LMSADMIN@atf.gov with login information and a temporary administrator password. Please login to the administrator site and change your password immediately.

If you have any questions or problems related to logging into the LMS administrator site or how to perform specific administrator functions, please call the EDS help desk at 1-877-875-3723 and identify yourself as a LMS Training Coordinator or Training Records Manager. If the help desk is unable to assist you, a ticket will be escalated to a member of the Learning Technologies Branch.

Rules of Behavior for LMS Training Coordinators, Training Records Managers and Help Desk Staff

In addition to the Rules of Behavior and Customer Agreement for ATF Workstation Users (ATF P 7500.1), the following Rules of Behavior are in effect for users of the LMS Administrator site to ensure the integrity and safety of user and training data.

Accounts and Passwords

The user name and password assigned to you are for your exclusive use. Do not share your user ID and password with anyone. Do not use anyone else's user ID and password to logon or

perform transactions in the LMS on that person's behalf -- with or without the other person's explicit or implicit permission. Do not write your password down, store it on your computer, or allow your Internet browser to save the password.

In the event your responsibilities for managing and/or coordinating training, or answering LMS related help desk questions changes, you must submit an e-request immediately so that your system access can be adjusted accordingly. All changes to roles and domain restrictions must be documented through the completion of an e-request.

Transactions in the system are tracked by user ID. You will be held strictly accountable for any transaction initiated in the LMS with your user name. Abuse of privileges may result in the revocation of your access rights to the application.

To prevent unauthorized access, you should always logout of the LMS and close your browser when you are finished using the application, or when you have to leave your computer.

Data Access and Functional Responsibilities

As a Training Records Manager, Training Coordinator or Help Desk employee, you are assigned the minimum level of data and functional access needed to perform your job responsibilities and functions. However, in some cases, you may have access to users or training data that you are not directly responsible for managing. Do not perform any transaction in the LMS on records that fall outside your scope of responsibility.

Output

Take the same care with system output (printed reports or saved data files) as with the system itself. Control all access to printouts, files, and disks that contain sensitive information. All output from the LMS should be considered "Sensitive but Unclassified (SBU)."

- Lock up printed copies and/or disks containing sensitive information at the end of the day or when otherwise unattended.
- Do not leave printed reports containing sensitive information unattended at printers.
- Mark media with the type of sensitive information they contain.
- Dispose of disks with sensitive information by erasing sensitive data, shredding, or following other appropriate procedures.
- Abide by procedures governing the channels for disseminating information by sharing printed or exported data only with others with a valid "need-to-know."

LMS Accounts for Training Coordinators, Training Records Managers and Help Desk Staff

Reporting Suspected or Known Security Violations

Failure to comply with the above *mandatory* rules of behavior will be considered a security incident. If the incident is deemed willful, it will be escalated to a security violation. Depending on the number of security violations and the sensitivity of the information involved, disciplinary actions for such violations may consist of a letter of warning/caution, a suspension, or removal from Federal Service.

Report any security incident, whether real or perceived, or any suspected fraud or abuse to the ATF Help Desk at 877-875-3723. If required, they will refer you to the Information Systems Security Office.

LMS Accounts for Training Coordinators, Training Records Managers and Help Desk Staff

CERTIFICATION STATEMENT

This is to certify that the below named individual has read, understands, and will comply with the Rules of behavior for LMS Training Coordinators, Training Records Managers and Help Desk Staff.

Date:

Printed/Typed Name:

Account Type: ☐Training Coordinator ☐Training Records Manager ☐ Help Desk

User/ATF Login ID:

Email Address:

Office:

Organizational Code:

Last 4 digits of Social Security Number:

User's Signature:

DSO's Signature:

After reading, please sign and fax this final page to: 202-648-9718.

Revised: February 2011