

Procedure Document

Category: Training
Description: Tracking Information Technology Security Awareness Training for Short-Term
Emergency Response Personnel
Policy Origin: OMB A-130, Appendix III
Revision Date: <date>

Purpose: Users of Department of the Interior (DOI) computer systems are required to read and acknowledge their understanding of the DOI's statement of information technology (IT) security awareness and individual user responsibilities. They are subsequently required to take and pass the Federal Information Systems Security Awareness (FISSA) training within the required timeframe. Many seasonal, non-federal employees assigned during the fire season are on-site for two weeks or less. For these individuals, it was determined that a streamlined procedure for fulfilling security awareness was needed. This is accomplished by using a combination of the *IT Security Awareness and Best Practices* handout and a user log that tracks individual user's statements that they agree to adhere to the identified IT security best practices.

Scope: All short-term emergency response personnel who use DOI computer systems.

Oversight Responsibility:

The benefiting activity manager is responsible for ensuring that all short-term emergency response personnel under their purview follow these procedures. The manager may assign IT support personnel to distribute user accounts and coordinate with the local Help Desk to reset accounts when no longer needed. The manager also makes the user log available at all times for IT support personnel to review as needed. IT support personnel shall distribute User ID's and initial logon passwords in a sealed envelope.

Steps:

1. Each short-term emergency response personnel are provided a copy of the *IT Security Awareness and Best Practices* handout **before** they are granted initial access to their account.
2. The user reads the *IT Security Awareness and Best Practices* handout and contacts IT support personnel or the IT Security Manager if they have any questions. This is critically important in order to ensure that the user is aware of their responsibilities and to provide bureau/office accountability.
3. The user fills out the *User Log for Short-Term Emergency Response Personnel* and signs it to acknowledge their agreement to follow DOI IT security best practices. The Coordinator on Duty initials the log signifying that the individual signed this acknowledgement.
4. The IT support personnel inserts the user ID and initial logon password into a sealed envelope.
5. The user receives the sealed envelope.

