Rules of Behavior for Functional Managers

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mba_060106_cd44

Information System Security
Rules of Behavior
for Functional Managers

Table of Contents

Information Systems Security
Functional Managers Rules of Behavior

1. Rules of Behavior Overview

Within ADS 545, five NIST-defined roles have corresponding rules of behavior (ROBs). These five roles are User, System Administrator, Information System Security Officer (ISSO), Functional Management, and Executive Management. User rules of behavior apply to all USAID personnel who use information systems. The other four roles have rules of behavior that are specific to their classification alone, and that will take precedence over the rules of behavior defined for the User role.

2. User Responsibilities

Users are individuals who are authorized by privilege to use information system and networks. A user can also be an individual who uses information processed by any information system.

3. User Rules of Behavior

This section contains the Rules of Behavior (ROB) as derived from the policies contained in **ADS 545, Information System Security Policy**.

This set of ROB supplements the User ROB. The rules contained in this document take precedence over the User ROB when there is a conflict with specific rules. If you have questions about the ROB please contact your local ISSO or CISO's office.

You must sign and return an acknowledgement for each copy of the ROB that you are responsible for based upon your role(s). The acknowledgement page(s) indicates that you have received, read, and that you understand your responsibilities as a user of USAID General Support System information systems. You further agree to follow the rules of behavior and understand that you may be subject to the penalties specified in **ADS 545** for infractions of the rules of behavior.

The ROB may reference other documents such as policy, standards, procedures, guidelines or other related items.

3.1 System Development Life Cycle (SDLC) Planning

a. You must conduct a system security and data sensitivity assessment for each information system under development.

b. You must conduct a privacy impact assessment before

- developing or procuring IT systems;
- developing projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or
- initiating a new electronic collection of information in identifiable form for 10 or more persons, consistent with the **Paperwork Reduction Act** (excluding agencies, instrumentalities or employees of the federal government).

c. For each USAID information system, you must select the appropriate managerial, operational, and technical controls to maintain security at the level to which the information system was assessed.

d. The System Owner must identify and track all security requirements within a system-level configuration management system.

3.2 Information Assurance

3.2.1 Certification and Accreditation (C&A)

a. You must conduct an initial certification and accreditation for each information system, and successfully receive an authority to operate (ATO) or an interim authority to operate (IATO) before deploying the information system to production.

b. You must conduct subsequent certifications and accreditations once every three years, or whenever the system, or its operating environment, significantly changes.

3.2.2 Annual Security Review

a. You must conduct annual security reviews against each information system's access privileges and operating practices.

b. You must conduct annual, periodic testing and evaluation of the security procedures and security controls to determine their effectiveness.

3.2.3 System Testing and Evaluation (ST&E)

You must evaluate annually the information system security controls, to determine whether the controls sufficiently mitigate risk to maintain operational status.

USAID-stated procedures for conducting these three information assurance processes are contained in **Information Assurance Procedures**.

3.3 Personnel

The following rules govern functional management's responsibilities for management of the people who use, develop, operate, maintain, and support USAID's information system.

3.3.1 General Personnel Policies

a. For each position, USAID Functional Management must incorporate the security functions required for that role into the position description for that position. Each position must be developed around the security tenets of individual accountability, least privilege, separation of duties, and need to know.

b. Potential staff must successfully complete a background checks **or** an employment eligibility forms before System Administrators grant them access to any USAID system.

3.3.2 Staffing

a. For each USAID system, you must maintain a roster of key technical positions and the individuals who fill them. The roster must be included in the System Security Plan for the information system.

b. You must cross-train staff who fill critical roles to provide redundancy for the functions that those positions perform.

3.3.3 User Administration

a. The CISO must establish and maintain generic Computer Security User Account Management Procedures (Reserved).

b. You must establish a user account management system, which can be used to handle access control changes, for each information system.

c. You and System ISSOs must establish security controls and procedures to govern user administration functions for their system(s).

Personnel procedures are contained in Personnel Security Procedures (Reserved).

User account management procedures are contained in Computer Security User Account Management Procedures (Reserved).

3.4 Business Continuity Planning and Disaster Recovery Planning

3.4.1 Business Continuity Planning

a. You must develop business continuity plans for each system.

b. You must annually test business continuity plans for each system.

3.4.2. Disaster Recovery Planning

a. You must develop disaster recovery plans for each system.

b. You must annually test disaster recovery plans for each system.

The CISO-established, USAID basic business continuity planning procedures are stated in **Business Continuity Planning Procedures and Guidelines**.

The CISO-established, USAID basic disaster recovery planning procedures are stated in **Disaster Recovery Planning Procedures and Guidelines**.

3.5 Awareness and Training

3.5.1 Awareness

If you and System ISSOs have developed system-specific awareness materials for their information system, staff must receive it before they are given access to the information system.

3.5.2 Training

a. The CISO, System ISSO, System Owner or System Administrator must provide remedial training to users who cause a security incident, after the incident occurs.

b. If you and System ISSOs have developed system-specific training for their information system, staff must receive it before they are given access to the information system.

3.6 User Support

The following policy states that USAID must establish a user support capability to generate an initial response and react to a reported security incident.

You and ISSOs must document information system-specific help desk and incident handling procedures in their information systems' System Security Plans.

3.7 Software Support

3.7.1 General Software Support

a. You and ISSOs must implement security controls on your information systems, or use a capability provided by the CISO or the GSS ISSO, to detect changes to software on each system.

b. You and System Administrators must only attach workstations that are configured with the standard USAID desktop image to the USAID network.

USAID stated virus detection guidelines are contained in **Virus Detection Guidelines**.

3.8 Software Development and Maintenance

3.8.1 Software Development

a. You must maintain a separate development environment for the information systems. USAID production environments, including AIDNET, must not be used for any development activity.

b. You must ensure that software unnecessary for production server operation (e.g., compilers, debuggers, and utilities) is removed from production servers.

c. You and ISSOs must document all software features and functions that constitute the information system security controls.

3.9 Configuration Management

a. You must develop and use configuration management procedures for all production information systems.

b. You must maintain an accurate inventory of system software, hardware and configurations.

3.10 Backups

The following policy states USAID's position on server and workstation backup management, handling, and creation. Backups are the process in which a duplicate copy of software, files, information/data is made on a second medium (a disk or tape) as a precaution in case the original is lost or corrupted. Backups are an important step to preventing information/data loss.

You must create backup plans for each information system.

4. Technical Policies

4.1 Identification and Authentication (Passwords)

a. You must configure security controls so that users are identified and authenticated, using UIDs and passwords, or similar authentication mechanism, prior to being granted access to any USAID information system.

b. You and System ISSOs must establish security controls and handling procedures for passwords specific to their system. System Administrators must implement these security controls.

Password creation standards are contained in **Password Creation Standards**.

4.2 Audit Trails and Logs

a. The CISO must establish minimum standards for audit logging.

b. You must establish rules for audit logging, which the CISO must review and approve.

c. You must forward data captured in audit logs to the CISO as requested.