Rules of Behavior for Executive Management

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545maz_060106_cd44

Information System Security
Rules of Behavior
for Executive Management

Table of Contents

Information Systems Security
Executive Management Rules of Behavior

1. Rules of Behavior Overview

Within ADS Chapter 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 systems 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 you 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.

4. Broad Organizational Rules of Behavior

The following rules are global; they apply to all information security systems at USAID.

The Agency must specify a Record Retention Standard (RRS) for records retained to support information security policy (e.g., audit logs, incident reports, and computer forensics that support disciplinary actions, etc.).

4.1 Personnel

4.1.1 General Personnel Policies

a. For each position, USAID Executive 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. You must make certain that potential staff successfully completes background checks **or** an employment eligibility form~~s~~ before System Administrators grant~~s~~ them access to any USAID system.

4.1.2 Critical Technical and Human Threat Environments

The Regional Security Officer (RSO) must first approve Foreign Service Nationals (FSN) before they can hold an administrative position in a critical threat environment.

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

4.2 User Support

The Agency must establish a user support capability, such as a Help Desk, to support basic user security functions (e.g., password changes, anti-virus support, incident reporting, etc.).

5. Issue-Specific Policies

5.1 Critical Threat Postings

The mission Executive Officer (EXO) must request that the Regional Security Officer (RSO) perform the highest level background investigation available within the host country on Foreign Service Nationals (FSN) prior to employment.