Rules of Behavior for Users

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mbd_060106_cd44

Information System Security
Rules of Behavior
for Users

Table of Contents

Information Systems Security User 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 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 USAID User Rules of Behavior, organized within the framework established for the policies contained in **ADS 545, Information System Security**. This document contains the rules of behavior that govern user responsibilities.

You must sign an acknowledgement page that 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 Broad Organizational Rules of Behavior

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

a. You must adhere to this security policy contained in **ADS 545**, and the plans, procedures, rules of behavior, standards, checklists, and guidelines derived from them.

b. You must use information systems only for USAID business or other limited, federally authorized use.

c. You must only process information on systems that are approved for processing at the same security level or higher than that of the information being processed.

d. You must not participate in unethical, illegal or inappropriate activities, such as, but not limited to, pirating software, stealing passwords, stealing credit card numbers, and viewing/exchanging inappropriate written or graphic material (e.g., pornography).

e. You have no reasonable expectation of privacy when using any USAID information systems. USAID will protect the privacy of specific personally identifiable information as required by law.

f. You must safeguard USAID information/data.

g. You must not bypass, modify, deactivate or intentionally probe security controls used to protect USAID's information systems without written approval from the CISO.

3.1.1 Penalties and Disciplinary Actions

The following policy states the potential consequences that may result from policy infractions committed by staff.

Staff who either intentionally or inadvertently misuse USAID automated resources or do not comply with the policies in **ADS 545** or with the plans, procedures and rules of behavior derived from them, may be subject to the full range of administrative disciplinary actions as defined in **ADS 485** or **ADS 487**, as applicable. These sanctions may include:

- Counseling, remedial training, revocation of access privileges, and possibly termination.
- Contractor employees can have their access privileges revoked; their contract itself could be partially terminated as a result of an infraction.
- Where such actions appear to be criminal in nature, the matter must be referred to the appropriate Assistant U.S. Attorney by the USAID Inspector General.

3.1.2 Rules of Behavior

The following rules govern user responsibilities for the rules of behavior document.

You must acknowledge, in writing, receipt of the ROBs for each system to which you will be granted access, prior to accessing each system.

3.1.3 Privacy Rules

The following policies state the responsibilities for personal information that is stored on USAID's information systems. Personal data is any information that can be individually identified – information that can be bound to the identity of a specific individual. Federal regulations require that personal information be protected from loss, disclosure, or any other unauthorized use.

a. You must not enter or store information protected under the **Privacy Act of 1974**, and any subsequent legislation, on any information system, except as required to fulfill an approved USAID objective or business function.

b. You must not monitor, access, or disclose an individual worker's communications or files without approval consistent with guidance from the USAID Office of the General Counsel, Senior Privacy Official, the CISO or others, as required by Federal regulations. Additionally, staff may not monitor, access or disclose personally identifiable information, unless:

- A legitimate business need exists that cannot be met by other means, or
- The involved individual is unavailable and timing is critical, or
- There is cause to suspect criminal activity or policy violation, or
- Monitoring is required by law, regulation, or third-party agreement.

3.2 Operational Rules

3.2.1 Incident Handling

a. You must immediately report suspected or known security incidents as directed in the **Incident Identification and Reporting Procedures**.

b. You must follow incident handling procedures as directed by USAID personnel responsible for information security.

The USAID basic incident handling procedures, developed by the CISO, to comply with the US-CERT processes, are contained in **Incident Identification and Reporting Procedures**.

3.2.2 Awareness and Training

3.2.2.1 Awareness

You must participate in the CISO information security awareness program as required by Federal regulations.

3.2.2.2 Training

If you have security responsibilities you must maintain your security training by taking information security specific training as required by Federal regulations.

3.2.3 Software Development and Maintenance

3.2.3.1 Software Development

If you develop software, you must not develop software for USAID that incorporates "backdoors", deactivation mechanisms, and other undocumented functions that could be used to compromise security.

3.2.3.2 Software Maintenance

You must not use hardware or software for testing information system vulnerabilities.

3.2.4 Physical Facilities and Restricted Spaces

3.2.4.1 Restricted Space (Server Rooms, Telecommunications Closets, etc.)

a. You must follow restricted access procedures, including signing in and properly escorting visitors.

b. If you are on the authorized access list for a restricted space, then you may escort individuals within that restricted spaces.

c. If you are not on the authorized access list for a restricted space, then you must sign a visitor's log (prior to admission), be escorted and monitored by staff on the authorized access list while in the restricted space.

Physical facilities and restricted spaces security procedures are contained in **Restricted Access Procedures and Guidelines**.

3.2.5 Networks and Workstation Connectivity

3.2.5.1 Networks

a. You must follow established network access procedures.

b. You must be identified and authenticated prior to accessing the network.

c. You must not use network monitoring and testing equipment.

d. You must not publicly release any information about USAID networks without the approval of the CISO, the GSS ISSO, or their System ISSO.

e. You must not alter the USAID network by changing settings for network devices or by adding or removing equipment to the USAID network.

f. You must not use modems, 802.11, Bluetooth or other wireless devices unless CISO-approved.

3.2.6 Media Controls

3.2.6.1 Media Usage

a. You must follow established procedures for media usage and handling.

b. You must follow CISO-approved data remanence procedures.

c. You must securely store all removable media when not in use.

3.2.6.2 Transporting Media

a. You must follow established guidelines when transporting media.

Media handling procedures are contained in **Media Handling Procedures and Guidelines**.

Data remanence procedures are contained in **Data Remanence Procedures**.

3.2.7 Backups

You must comply with backup procedures for information, contained on your workstation(s).

3.2.8 Information Sharing

You must follow established disclosure guidelines when releasing information.

Related information may be found in the following documents:

- **ADS 507, Freedom of Information Act (FOIA),**
- **ADS 508, Privacy Act 1974,**
- **ADS 509, Creating, Altering, or Terminating a System of Records,**
- **ADS 557, Public Information,**
- **ADS 558, Public Activity,**
- **ADS 559, Inquiries from the News Media,** and
- **ADS 560, News Releases and Services.**

3.2.9 Intellectual Property Management

a. All information processed, generated or stored on any USAID information system is the property of USAID.

b. If you work with USAID-specific intellectual property, while using any USAID information system, you must sign a **non-disclosure agreement (NDA)**.

c. If you work with third-party intellectual property while employed by USAID, using any USAID information system, you must sign an NDA with the third party when requested to do so.

d. Whenever you use, store, or distribute copyrighted materials within a USAID information system, you must use a citation. Where possible, you must obtain the permission of the author/owner to use the material.

3.3 Technical Policies

3.3.1 Identification and Authentication (Passwords)

a. You must not write down passwords unless they are stored in a CISO-approved secure container.

b. You must not share your passwords.

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

3.3.2 Logical Access Controls

You must follow the password standards outlined in the **Password Creation Standards** document.

3.3.3 Collaboration Software

a. You must not install collaboration software unless approved by the IRM CCB and CISO.

b. You must not use collaboration software unless approved by the IRM CCB and the CISO.

c. You must disable any remote control capability in collaboration software not approved by the CISO.

3.3.4 Cryptography

You must follow CISO-established standards and guidelines when selecting an encryption technology for a USAID information system.

3.3.5 E-Mail

You must follow the standards and procedures outlined in the acceptable e-mail use document. The E-mail acceptable use policy is contained in **E-Mail Acceptable Usage Policy**.

Additional information may be found in **ADS 541, Information Management**.

3.3.6 File Sharing Software

a. You must not install file sharing software unless approved by the IRM CCB and the CISO.

b. You must not use file sharing software unless approved by the IRM CCB and the CISO.

3.3.7 Freeware

You must not install freeware on any USAID information system unless approved by the IRM CCB and the CISO.

3.3.8 Instant Messaging (IM)

a. You must not install instant messaging software unless approved by the IRM CCB and the CISO.

b. You must not use instant messaging software unless approved by the IRM CCB and the CISO.

c. You must disable instant messaging software remote control from other workstations.

d. You must not use any software or web browsers, for instant messaging.

3.3.9 Internet and Intranet Usage

You must follow the guidelines outlined in the acceptable use policy for the Internet and intranet. The Internet acceptable use policy is contained in the **Internet Acceptable Usage Policy**.

Additional information may be found in **ADS 541, Information Management**.

3.3.10 Internet Radio

a. You must not listen to internet radio using any USAID resource unless approved by the IRM CCB and/or the CISO.

b. You must not listen to internet radio using any USAID resource unless approved by the IRM CCB and/or the CISO.

3.3.11 Mobile Computing Devices

a. You must follow the **Mobile Computing Standards and Guidelines**.

b. You must not connect non-USAID-issued computing device(s) to the USAID network or information systems.

c. You should not connect USAID-issued computing device(s) to non-USAID networks or Internet service providers (ISPs), if the devices cannot be configured with anti-virus and firewall software. When connected to non-USAID networks, the anti-virus and firewall software should be operational.

Mobile computing standards and guidelines are contained in **Mobile Computing Standards and Guidelines**.

3.3.12 Open Source

You must not install open source software unless approved by the IRM CCB and the CISO.

3.3.13 Peer-to-Peer Software

a. You must not install peer-to peer software unless approved by the IRM CCB and the CISO.

b. You must not use peer-to peer software unless approved by IRM CCB and the CISO.

3.3.14 Remote Control Software

a. You must not install remote control software unless approved by the IRM CCB and the CISO.

b. You must not use remote control software unless approved by the IRM CCB and the CISO.

3.3.15 Shareware

a. You must not install shareware unless approved by the IRM CCB and the CISO.

b. You must not use shareware unless approved by the IRM CCB and the CISO.

3.3.16 Spyware and Adware

You must not alter or disable spyware or adware detection software on any workstation or laptop.

3.3.17 Virtual Private Network (VPN)

Staff using VPN technology to connect to USAID systems must follow the CISO-established standards.

3.3.18 Wireless Access

a. You must identify yourself and be authenticated prior to accessing the network via wireless connection

b. You must comply with established network policies once a wireless connection has been established. The wireless access standards are contained in **Wireless Access Standards and Guidelines**.