Rules of Behavior for System Administrators

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mbc_060106_cd44

Information System Security
Rules of Behavior
for System Administrators

1. Rules of Behavior Overview 2
2. User Responsibilities 2
3. User Rules of Behavior 2
4. User Support 2
5. Software Support 3
6. Software Maintenance 3
7. Networks and Workstation Connectivity 3
8. Firewalls 3
9. Production & Development Servers 4
10. System Maintenance 4
11. Backups 5
12. Mobile Computing Devices 5
13. Wireless Access 5
14. Internet Protocol Version 6 (IPv6) 5

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 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.

4. User Support

a. You, the Help Desk, and information security staff must follow incident reporting procedures, developed and documented by the CISO, the GSS Security Operations Staff, and System ISSOs, and must act immediately if a security incident is reported.

b. You and the Help Desk must document all reported security incidents, as specified in the USAID basic or system-specific incident reporting procedures.

5. Software Support

a. General Software Support

1. You may only attach workstations that are configured with the standard USAID desktop image to the USAID network.

2. You must install only approved software on any USAID information system.

b. Protection against Malicious Software

You and the Help Desk must follow the established procedures for detecting viruses, Trojans, and other types of malicious software.

6. Software Maintenance

a. You must follow established procedures for implementing fixes, patches, and scripts for software.

b. With CISO approval, you may use hardware or software for testing information system vulnerabilities.

7. Networks and Workstation Connectivity

a. You must configure access controls to network devices to limit or restrict traffic to and from the USAID network.

b. You must deploy and use USAID-approved time servers.

c. You must not further implement or expand the~~ir~~ use of Dynamic Host Configuration Protocol on any USAID network without the express permission of the IRM CCB.

8. Firewalls

a. You must follow established firewall standards and procedures.

b. You must regulate all traffic traveling between lesser trusted networks, to include the Internet, and the USAID network, by passing it through a firewall.

c. You must validate new firewall configurations, and the GSS ISSO and the IRM CCB must approve the new configuration before production deployment.

d. You must run firewalls on dedicated machines.

e. You and the GSS ISSO must evaluate and approve all new firewalls and new connectivity paths for security risks.

f. You must log all changes to firewalls.

g. You and the GSS ISSO must periodically review firewall logs to check for anomalies.

h. You must maintain and respond to current information about firewall vulnerabilities. Firewall vulnerability information may be obtained from user groups, manufacturer's web pages, etc.

i. You must conduct, on a quarterly basis, or as prescribed by the CISO, a firewall "check" to make sure that old rules are disabled or removed and that the firewall policy has been reviewed.

9. Production & Development Servers

a. You must configure servers to conform to internal server security standards.

b. You must place Internet-accessible servers in a De-Militarized Zone (DMZ), e.g., web, e-mail, etc.

c. You and the System ISSO must evaluate all new servers and their interconnections for security risks.

10. System Maintenance

a. You must remove default accounts, where possible. If not possible, System Administrators must deactivate default accounts. Such accounts are typically used for system maintenance.

b. You must configure or restrict (e.g., through strong authentication, remote callback, etc.) access to remote diagnostics so that they can only be used to provide support services, and are disabled when not in use.

c. You must follow established data remanence procedures for data storage devices submitted for off-site maintenance.

d. You must restrict those who perform maintenance and repair activities on USAID systems to maintenance personnel who are 1) either direct-hire federal employees or 2) who are working under a contractual arrangement that includes the appropriate security

provisions in accordance with this chapter or **ADS 552 Classified Information Systems Security**.

11. Backups

You must implement and validate the backup plans for your information systems.

12. Mobile Computing Devices

You must examine any USAID-issued computing device, before it is directly connected to the USAID network. If the mobile computing device is found to be insecurely configured or compromised, you may extract the data from the device and must rebuilt it before connectivity to the USAID network is permitted.

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

13. Wireless Access

You must only install CISO-approved wireless devices.

The wireless access standards are contained in **Wireless Access Standards and Guidelines**.

14. Internet Protocol Version 6 (IPv6)

You must follow CISO-established standards and guidelines for IPv6. The IPv6 Plans and Standards are located in **Internet Protocol Version 6 (IPv6) Plans and Standards**.