USAID
FROM THE AMERICAN PEOPLE

Rules of Behavior for Users

A Mandatory Reference for ADS Chapter 545

Partial Revision Date: 08/01/2013
Responsible Office: M/CIO
File Name: 545mbd_080113

Table of Contents

Text highlighted in yellow indicates that the material is new or substantively revised.

1. RULES OF BEHAVIOR (ROB) OVERVIEW

The following Rules of Behavior (ROB) apply to all users of applications, systems, and Information Technology (IT) resources managed by the United States Agency for International Development (USAID), as well as to all persons with access to personally identifiable information (PII) collected, used, maintained, and disseminated by USAID. Examples of such resources include government-issued laptop computers and mobile computing devices (MCDs). MCDs include, but are not limited to, personal digital assistants (PDAs) (e.g., Palm Pilots), smart phones, iPads, and plug-in and wireless peripherals which employ removable media (e.g., CDs, DVDs). MCDs also encompass USB flash memory (thumb) drives, external drives, and diskettes.

The ROB document is consistent with IT security policy and procedures within **ADS 545, Information Systems Security**, **ADS 508, USAID Privacy Policy**, **OMB Circular No. A-130, Revised, Management of Federal Information Resources, Appendix III**, and **NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Information.**

The ROB document applies to users at their primary workplace, alternative remote workplaces (e.g., telecommuting from home or from a satellite site) or any off-site work spaces (e.g., working while traveling, etc.).

Misuse, whether intentional or unintentional, or failure to comply with these rules for Direct Hire employees may result in appropriate corrective measures, following due process, in accordance with **ADS 485, Disciplinary Action - Foreign Service** and **ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service**. For Non-USAID employees, contractors, and others working on behalf of USAID, one or more of the following disciplinary actions may apply: verbal warnings or counseling, written warnings or counseling, revocation of privileges, termination of employment, and/or removal from a contract supporting USAID. Where such actions appear to be criminal in nature, the matter will be referred to the appropriate Assistant U.S. Attorney by the USAID Inspector General for action.

Users must acknowledge receipt of ROB by signing the signature page of this document, prior to accessing USAID information systems.

2. USER RULES OF BEHAVIOR

This section contains the system user ROB as derived from the policies contained in **ADS 545, Information Systems Security,** and **ADS 508, USAID Privacy Policy.**

2.1 SYSTEM ACCESS

- I understand that I am given access to only those systems for which I require access to perform my official duties.
- I will not attempt to access systems I am not authorized to access.
- I must only access information necessary to perform my official duties or if there's an official need-to-know.

- I must ensure that my assigned laptops and MCDs are secured and encrypted to minimize loss of sensitive or confidential information.
- I must not connect non-USAID-issued MCDs, including storage devices, to the USAID network or information systems.
- I must immediately notify the system administrator when there is a change in my employee status and/or access to the system is no longer required.

2.2 PASSWORDS AND OTHER ACCESS CONTROL MEASURES

- I must choose passwords, which meet the complexity requirements described by the respective System Administrators (SAs) or **ADS 545** policy. Specific standards are defined in **Password Creation Standards and Technical Controls**.
- I must protect passwords and access numbers from disclosure. I must not record passwords or access control numbers on paper or in electronic form and store them on or with USAID workstations, laptop computers, or MCDs.
- To prevent others from obtaining my password via "shoulder surfing," I must shield my keyboard from view as I enter my password.
- I must not use passwords such as dictionary words, proper nouns, names of any person, pet, child, or fictional character.
- I must not use an employee serial number, social security number, birth date, phone number, remote access serial number, or information about myself that could be easily guessed as a User ID for any USAID system.
- If issued a remote access token, I must not write down the token pin on the token hardware.
- If compromise of a password is known or suspected, I must promptly change that password and report the incident.
- I must not attempt to bypass access control measures.
- I must not share passwords.
- I must check with my team lead for all other password rules that pertain to my group.
- If passphrases are used in addition to, or instead of, passwords, I must follow the same guidelines.
- My passwords must contain a combination of alphabetic, numeric, and special characters.
- My passwords must not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123."
- My passwords must not be any word, noun, or name spelled backwards or appended with a single-digit or with a two-digit "year" string, such as 98xyz123.

2.3 DATA PROTECTION

- I must restrict disclosure of USAID information to those who have a business need and are authorized to receive the information.
- I must ensure that USAID information is stored on Government Furnished Equipment (GFE). GFE is property that is acquired directly by the government and then made available to the employee for use.
- I must store all work-related files on the approved network resources. I understand that according to USAID operational policy, only data stored on the approved network resources will be automatically backed up by the CIO, documents saved locally to desktop and laptop computers will not be backed up by the CIO.
- I must not store USAID sensitive information on personal equipment.
- I must not send and/or store USAID sensitive information to a personal e-mail account.
- I must protect sensitive information from disclosure to unauthorized persons or groups.
- I must take every precaution to prevent unauthorized individuals from observing display output. (Use privacy screens, keep computer screens from facing windows or doors, etc.)
- I must log off or lock my workstation or laptop computer, or I must use a password-protected screensaver, whenever I step away from my work area, even for a short time.
- I must completely LOG OFF whenever I am away from my computer for more than two hours.
- I must not access, process, or store classified information on USAID office equipment that has not been authorized for such processing.
- I must ensure that USAID information is properly disposed of when a business need no longer exists. (See **ADS 502, USAID Records Management Program**.)
- I must not use the USAID systems for data mining unless explicitly authorized to do so.
- I must not communicate sensitive or classified information over, nor store such information in, voice mail.

2.4 PII PROTECTION

- I must protect PII in all formats, including oral, paper, and electronic formats.
- I must protect PII against unauthorized access or disclosure by ensuring that only those people who have a clearly demonstrated need to know or use the PII are given access.
- I must mark and handle PII as Sensitive But Unclassified (SBU).
- I must maintain a high level of confidentiality, protection, and respect for PII data.

- I must secure paper and mobile media with PII in locked a drawer or cabinet.
- I must not leave PII on a desk, printer, fax machine, or copier.
- I must store PII only on devices encrypted via USAID-approved encryption software.
- I must use encryption when sending PII by email (Adobe Acrobat or WinZip).
- I must not use PII obtained from USAID on my personal computer, mobile device, or email.
- I must check for PII in email strings and attachments before sending email outside of USAID approved domains, which include only usaid.gov, state.gov, ofda.gov, and oti.gov.
- I must refer all external requests for access to PII to the USAID Freedom of Information Act (FOIA) Office at **foia@usaid.gov**.
- I must report immediately upon discovery *all potential and actual* privacy breaches to the CIO Helpdesk at 202-712-1234 or **CIO-HELPDESK@usaid.gov** ***and*** the Privacy Office at **privacy@usaid.gov**, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred.
- I must destroy PII in paper format by shredding
- I must store and destroy PII on electronic media according to the **Media Handling Procedures and Guidelines**.

2.5 MEDIA USAGE AND CONTROL

- I must follow established procedures for media handling.
- I must follow CISO-approved data remanence procedures.
- I must securely store all removable media when not in use.
- I must follow established guidelines when transporting media.

Media handling procedures appear in **Media Handling Procedures and Guidelines**.

Data remanence procedures appear in **Data Remanence Procedures**.

2.6 INFORMATION SHARING

I must follow established disclosure guidelines when releasing information.

Related information may be found in the following documents:

- **ADS 507, Freedom of Information Act,**
- **ADS 508, USAID Privacy Policy**
- **ADS 557, Public Information**
- **ADS 558, Public Activity**
- **ADS 559, Inquiries from the News Media**, and

- **ADS 560, News Releases and Services**.

2.7 INTELLECTUAL PROPERTY MANAGEMENT

- All information processed, generated, or stored on any USAID information system is the property of USAID.
- If I work with USAID sensitive data while using any USAID information system, I must sign a Non-Disclosure Agreement (NDA) when requested to do so. (See **AID Form 545-5, USAID Sensitive Data Nondisclosure Agreement**.)
- If I work with third-party intellectual property while employed by USAID, using any USAID information system, I must sign a NDA with the third party when requested to do so.
- Whenever I use, store, or distribute copyrighted materials within a USAID information system, I must use a citation to credit the author. Where possible, I must obtain the permission of the author/owner to use the material.

2.8 USE OF GOVERNMENT IT EQUIPMENT

- I must comply with USAID policy regarding personal use of USAID office equipment. I understand that USAID office equipment (including printers, copiers, scanners, fax machines, servers, email and internet access, applications, and workstations) is to be used for official use, with only limited personal use allowed. (See specific guidance in **ADS 541, Information Management**.**)**
- I must adhere to the USAID guidelines for unacceptable access, storage or sharing of material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. Access and sharing of such information via email, bulletin board systems, chat groups, newsgroups, or instant messenger is prohibited. Users encountering or receiving this kind of material should immediately report the incident to either the USAID Help Desk or ISSO.
- I understand that my use of USAID IT equipment may be monitored, and I consent to this monitoring.
- I must use only Agency-approved Universal Serial Bus (USB) removable storage devices unless explicitly approved by the CIO.
- I must not alter any GFE equipment, software, or configuration unless explicitly authorized to do so by the Chief Information Officer (CIO).
- I understand that personal files stored on GFE (e.g., workstations, laptops, MCDs) are stored at my own risk.
- I must return all USAID issued equipment upon leaving the agency.

2.9 SOFTWARE

- I must comply with all software licenses, copyrights, and all other local laws and regulations governing intellectual property and online activities. Anything posted on the Internet that is an original work may be protected by copyright laws (whether or not explicitly indicated). Users may not use copyrighted work without the author's permission.
- I must not install or use software unless approved by the change control board (CCB).
- I understand instant messaging and peer-to-peer software is prohibited from use on GFE unless explicitly approved by the CIO.

2.10 INTERNET AND EMAIL USE

- I understand that my internet and email use is for official use, with limited personal use allowed. Acceptable use guidance appears in documents as follows:
  - **Information Policy**.
  - **E-Mail Acceptable Usage Policy**.
  - **Internet Acceptable Usage Policy**.
- I understand that my internet and email use may be monitored, and I consent to this monitoring.
- Internet streaming (radio and video) is prohibited on USAID systems unless approved by the CIO.

2.11 INCIDENT REPORTING

- I must immediately report IT security incidents. Incidents must be reported to one of the following support teams:
  - USAID Help Desk by phone at (202) 712-1234 or by email at **CIO-HELPDESK@usaid.gov**.
  - USAID ISSO by email to **ISSO@usaid.gov**.
- Incident reporting standards can be found in the **Incident Identification and Reporting Procedures**.
- I must report immediately upon discovery *all potential and actual* privacy breaches to the CIO Helpdesk at 202-712-1234 or **CIO-HELPDESK@usaid.gov** ***and*** the Privacy Office at **privacy@usaid.gov**, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred.
- Incident reporting standards can be found in the Privacy Breach Response and Reporting section of **ADS 508**.

2.12 PHYSICAL ACCESS AND ACCESS TO RESTRICTED SPACES

- I must protect my building access badge(s), computer user ID, password, access tokens, and other USAID access mechanisms.
- I must follow restricted access procedures, including signing in and properly escorting visitors.
- Physical facilities and restricted spaces security procedures appear in **Restricted Access Procedures and Guidelines**.

2.13 TELECOMMUTING AND REMOTE ACCESS

- At my alternate workplace, I must follow security practices that are the same as or equivalent to those required of me at my primary workplace. These include print securely, face computer screen away from the window, protect passwords, view SBU information securely, etc.
- I must physically protect any GFE used for telecommuting, even when it is not in use.
- I must protect sensitive data at my alternate workplace. This includes properly disposing of sensitive information (e.g., by shredding).

2.14 LAPTOP COMPUTERS AND MOBILE COMPUTING DEVICES

- I must password-protect my Agency-issued MCDs including smartphones. I must set the security timeout for any MCD to the established timeout period.
- I must keep the laptop or MCD under my physical control at all times, or I must secure it in a suitable locked container.
- I must take all necessary precautions to protect MCDs including laptops against loss, theft, damage, abuse, or unauthorized use by employing lockable cases, keyboards and locking cables.
- I must keep antivirus software on the laptop up-to-date.
- I must comply with the requirement that sensitive information processed, stored, or transmitted on wireless devices and laptops computers must be encrypted using Agency approved encryption methods.
- I must take precautions to protect sensitive information that might be visible on my laptop monitor (e.g., use a privacy filte, sit with screen facing away from public view).

2.15 ACCOUNTABILITY

- I understand that I have no expectation of privacy while using any USAID equipment or while using USAID Internet or email services.
- I understand that I will be held accountable for my actions while accessing and using USAID systems and IT resources.

- I must report security violations, incidents, and vulnerabilities in one of the following ways:
  - USAID Help Desk by phone at (202) 712-1234 or by email at **CIO-HELPDESK@usaid.gov**
  - USAID ISSO by email at **ISSO@usaid.gov**.
- I must be responsible for reading and understanding the requirements for information that is SBU. See **Sensitive But Unclassified (SBU) Information 12 FAM 540 and 12 FAM 544 SBU Handling Procedure: Transmission, Mailing, Safeguarding/Storage, And Destruction**.

Note: Sensitive But Unclassified (SBU) definition and associated handling guidelines can only be found on the USAID office of Security website, Please contact **ads@usaid.gov** for assistance.

Acknowledgment Statement for Rules of Behavior

I acknowledge that I have read the Rules of Behavior, I understand, and must comply with them. I understand that failure to comply with these rules may result in appropriate corrective measures, following due process, for Direct Hire employees in accordance with **ADS 485** and **ADS 487**, and for contract employees one or more of the following actions may apply: termination of employment, verbal warnings or counseling, written warnings or counseling, revocation of privileges and/or removal from a contract supporting USAID. Where such actions appear to be criminal in nature, I acknowledge that the matter will be referred to the appropriate Assistant U.S. Attorney by the USAID Inspector General for action.

Name of User (printed): _____

User's Work Phone Number: _____

User's Work Email Address: _____

Bureau/Office/Division: _____

Contractor Company Name (if applicable): _____

Work Location or Address: _____

_____

Supervisor's Name: _____

Supervisor's Phone Number: _____

(For users who are neither direct hire employees nor Personal Services Contractors, include the following information regarding the Contracting Officer's Representative (COR) or Agreement Officer's Representative (AOR):

COR/AOR Name
(printed):_____

COR/AOR Office: _____ Phone: _____

_____ _____

User Signature Date

Filing:

Original (Signature Page Only) - Onsite ISSO/Human Resource Management
Copy – Individual, COR/AOR (if applicable)

545mbd_080113