Rules of Behavior for Users

A Mandatory Reference for ADS Chapter 545

Partial Revision Date: 01/22/2024
Responsible Office: M/CIO
File Name: 545mbd_012224

Table of Contents

1. RULES OF BEHAVIOR OVERVIEW 3

2. SYSTEM ACCESS AND USE 4

3. USE OF SOFTWARE 6

4. USE OF THE INTERNET, EMAIL, MESSAGING APPLICATIONS 6

5. PASSWORD AND PASSPHRASE REQUIREMENTS OR LOGIN/ACCESS REQUIREMENTS 7

6. DATA PROTECTION 9

7. PROTECTION OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION 10

8. INFORMATION SHARING 12

9. INTELLECTUAL PROPERTY MANAGEMENT 12

10. AUTHORIZED AND USAID SPONSORED SOCIAL MEDIA REPRESENTATION 13

11. INFORMATION TECHNOLOGY INCIDENT REPORTING 13

12. PHYSICAL ACCESS AND ACCESS TO RESTRICTED SPACES 14

13. TELEWORKING AND REMOTE ACCESS 14

14. PROTECTION OF COMPUTER RESOURCES 15

15. ACKNOWLEDGEMENT STATEMENT FOR RULES OF BEHAVIOR 16

1. RULES OF BEHAVIOR OVERVIEW

The Rules of Behavior (ROB) are applicable to the USAID workforce. The term "workforce" refers to individuals working for, or on behalf of,the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes Direct-Hire employees, Personal Services Contractors (PSCs), Fellows, Participating Agency Service Agreement (PASA), and institutional contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS 501, The Automated Directives System**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to **Homeland Security Presidential Directive -12 (HSPD-12)** and Information Security requirements.

This mandatory reference establishes USAID's Rules of Behavior that govern the appropriate use and protection of Agency information and information resources to ensure the security of information technology (IT) equipment, systems, and data as well as their confidentiality, integrity, and availability in compliance with **OMB Circular A-130, Appendix I § 4(h)(6) and Appendix I § 4(h)(7)**. This mandatory reference is consistent with Information Technology (IT) security policy and procedures in **ADS 545, Information Systems Security**, **ADS 552, Cybersecurity for National Security Information Systems**, **ADS 508, Privacy Program**, and **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020**.

This mandatory reference applies to users in their primary workplace, alternative remote workplaces (*e.g.,* teleworking from home or from a satellite site), and any off-site work spaces (*e.g.,* working while traveling, etc.).

Misuse, whether intentional or unintentional, or failure to comply with these rules by Direct-Hire employees may result in 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** or the **Federal Acquisition Regulation (FAR)** and **USAID Acquisition Regulation (AIDAR)** for PSCs. For non-USAID employees, contractors, and others working on behalf of USAID, corrective action may be taken in accordance with the appropriate mechanism under which they are working, including one or more of the following disciplinary actions: verbal or written warnings, counseling, revocation of privileges, including removed or reduced access to Agency IT systems and facilities, and/or removal from a contract supporting USAID. Suspected criminal activity will be referred to the USAID Inspector General and/or the Assistant U.S. Attorney for action.

Users must acknowledge receipt of the ROB by signing the signature page of this document, prior to accessing USAID information systems. Users must review all updates to the Agency Rules of Behavior annually as part of the mandated Agency-wide Cybersecurity Training, as required by **ADS 545**.

2. SYSTEM ACCESS AND USE

The following ROB regarding what users must and must not do are relevant to USAID system access and use.

Users must:

- Follow USAID's policy regarding personal use of Government Furnished Equipment (GFE) (including desktops, laptops, tablets, and mobile phones). GFE is property that is acquired directly by the Federal Government through M/CIO-approved acquisition vehicles and then made available to members of the workforce for use. USAID office equipment (including printers, copiers, scanners, fax machines, servers, email and internet access, applications, and workstations) will be used for official use, with only limited personal use allowed (see **ADS 545mam, Acceptable Use of Agency Information Technology Resources**).

- 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, including 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 Bureau for Management, Office of the Chief Information Officer (M/CIO) Service Desk or the Information System Security Officer (ISSO).

- Report security, privacy, and information security incidents in one of the following ways, in accordance with **ADS 508**, **ADS 545**, and **ADS 568, National Security Information Program**:

    - Contact the M/CIO Service Desk by phone at (202) 712-1234 or by email at **cio-helpdesk@usaid.gov**.

    - Contact the Office of Security, Information and Industrial Security Branch (SEC/IIS) by phone at (202) 712-0990 or by email at **secinformationsecurity@usaid.gov**.

- Read and understand the requirements for Sensitive But Unclassified (SBU) information (see **Sensitive But Unclassified (SBU) Information 12 FAM 540** and **12 FAM 544 SBU Handling Procedure: Transmission, Mailing, Safeguarding/Storage, And Destruction**). Note: SBU definition and associated handling guidelines can be found on the Office of Security, Counterterrorism and Information Security Division, Information and Industrial Security Branch (SEC/CTIS/IIS) website. Please contact **secinformationsecurity@usaid.gov** for assistance.

- Only access information necessary to perform their official duties or if there is an official need-to-know.

- Restrict disclosure of USAID information to those who have an official need-to-know to perform their duties and are authorized to receive the information.

- Take precautions to prevent unauthorized individuals from observing display output (*e.g.,* use privacy screens, keep computer screens from facing windows or doors, etc.).

- Immediately notify the System Owner, Executive Officer (EXO), or Administrative Management Staff/Executive Management Team Officer (AMS/EMT) when there is a change in your employee status and/or access to an IT system is no longer required. Contractor staff must immediately notify the COR who will then work with the System Owner, EXO, or AMS/EMT Officer.

- Return all USAID-issued IT equipment upon leaving the Agency.

- Understand and acknowledge that they have no expectation of privacy while using any USAID equipment or while using USAID systems, Internet, electronic messaging, or email services.

- Understand and acknowledge that use of USAID IT systems, networks, and equipment is subject to monitoring.

- Understand that they will be held accountable for their actions while accessing and using USAID systems and IT resources.

- Understand that electronic messaging and peer-to-peer software is prohibited for downloading and use on GFE unless explicitly approved by M/CIO, as installation of software on all GFE must receive M/CIO approval.

- Only download applications on GFE mobile devices from the Approved Mobile App List on the Agency Approved Product Catalog (https://usaiditsm.servicenowservices.com/sphome?id=product_list_new - this link may only be accessed via the Agency Intranet). See **ADS 508** for guidance on submitting a Software and Hardware Request to M/CIO. Users must understand that downloading unapproved mobile applications (e.g., apps) onto GFE (e.g., laptops, tablets, and mobile phones) is prohibited.

- Understand that personal files stored on GFE (*e.g.*, workstations, laptops, mobile devices, network drive locations, and cloud-based storage) are stored at their own risk and may be monitored and reviewed, including by the Agency Records Officer, to determine if the content should be retained and/or submitted to the National Archives as an official Agency record.

Users must not:

- Install, download, or agree to any terms of service when using an official USAID cloud-based application, or using software on any USAID IT device, including mobile devices, unless approved by M/CIO.

- Install or download any mobile application (app) onto any GFE unless the app has been approved for use and is in the Approved Agency Mobile App List in the Approved Product Catalog.

- Attempt to access systems they are not authorized to access.

- Connect non-USAID-issued mobile devices, including storage devices, to the USAID network or information systems.

- Access USAID approved cloud services (*e.g.,* USAID email, Google Drive, etc.) using a personal device unless you've logged in through the Remote Access VDI **https://remoteaccess.usaid.gov**.

- Alter any GFE equipment, software, or configuration.

3. USE OF SOFTWARE

The following ROB regarding what users must and must not do are relevant to USAID use of software.

Users must:

- Ensure that all terms and conditions on the official use of any website or cloud service complies with programmatic or USG requirements. For M/CIO approved websites/cloud services (*e.g.,* Google mail), user can assume that M/CIO has reviewed the terms and conditions. If the user is required to agree to any terms or conditions for official use of a website or cloud service that has not been approved by M/CIO, the user must consult with his/her cognizant General Counsel (GC) or Resident Legal Officer (RLO).

- Comply with all copyrights, and other applicable laws and regulations governing intellectual property and online activities. When unsure, user must consult with his/her cognizant GC or RLO.

- Comply with usage rights and restrictions and licensing terms when using USAID owned or approved software or partner software.

- Consult with the Office of General Counsel, as needed, if a user has questions about the applicability of any software licenses or restrictions attached to the

software.

Users must not:

- Use copyrighted work without the author's permission. Anything posted on the Internet that is an original work may be protected by copyright laws (whether or not explicitly indicated).

4. USE OF THE INTERNET, EMAIL, MESSAGING APPLICATIONS

The following ROB regarding what users must and must not do govern USAID use of the Internet, email, and messaging applications.

Users must:

- Understand that USAID email, messaging applications, and access to the Internet is intended for official use, with limited personal use allowed.

- Understand that government emails and text messages could be considered Federal records and in these instances are subject to Federal record-keeping requirements, including Freedom of Information Act (FOIA) and Privacy Act requests.

- Understand that they must use their government-issued email account to conduct official Agency business to the fullest extent possible. Understand that the use of non-official accounts, applications, or platforms, including personal email accounts or approved non-Government messaging applications should never be the primary means of conducting Agency business, and must only be used in accordance with **ADS 502, The USAID Records Management Program**.

- Understand that if they use non-USAID/official accounts, applications, or platforms, including personal email accounts or an approved non-Government messaging application to conduct official government business in line with the requirements of **ADS 502,** they must forward all communications to their official government email no later than 20 days after use of the unofficial or personal email, to be in compliance with Federal recordkeeping requirements.

Users must not:

- Use Internet streaming (audio and video) on USAID devices and networks unless it is for official Agency business (*e.g.,* Agency-sponsored live streaming event such as an Agency Town Hall, watching a Congressional hearing, or participating in an Agency-related virtual event (*e.g.,* conferences or training)).

- Use unapproved web-based or mobile applications to send or receive emails, text, or short message service (SMS) messages to conduct official Agency

business, unless otherwise authorized by M/CIO or in case of limited exceptional circumstances outlined in ADS 502.

- Use Internet, email, and social media for fraudulent or harassing messages, sexual remarks or the downloading and/or streaming of illegal or inappropriate materials (*e.g.,* pornography) in accordance with **ADS 545mam**.

- Transmit Not Releasable to Foreign Nationals (NOFORN) (**5 FAM 435**) information on non-government accounts, applications, or platforms as outlined in **ADS 502**.

5. PASSWORD AND PASSPHRASE REQUIREMENTS OR LOGIN/ACCESS REQUIREMENTS

The following ROB regarding what users must and must not do are relevant to USAID to protect access to computing resources.

Users must:

- Protect passwords and access control numbers (*e.g.,* PIN codes) from disclosure.

- Use the same guidelines for passwords when passphrases are used in addition to, or instead of, passwords.

- Use passwords that contain a combination of alphabetic, numeric, and special characters (see **ADS 545mau, Password Creation Standards** for additional guidance on passwords).

- Store passwords for classified information systems (*e.g.*, ClassNet or Joint Worldwide Information Communications Systems (JWICs)) in General Services Administration (GSA) approved safes authorized to store the highest level of the information permitted on that particular system.

- Promptly change a password that is suspected or known to be compromised and report the incident to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** (see the Information Technology Incident Reporting for guidance below on reporting classified spillage incidents).

- Check with the appropriate team lead for all other password rules that pertain to your group.

- Take measures to prevent others from obtaining password(s) via “shoulder surfing.” Shoulder surfing is a form of data theft where criminals steal personal information by observing victims when they're using devices such as ATMs, computers, kiosks, or other electronics. The term refers to thieves peering over

the shoulders of targets, waiting for them to inadvertently reveal confidential information that can lead to theft, identity theft, or fraud.

Users must not:

- Record or store passwords for classified information systems in electronic form in password manager apps or on paper, unless they're stored in a GSA approved safe.

- Record passwords, access control numbers, or remote access pin codes on paper or in electronic form, or store them on or with USAID workstations, laptop computers, mobile devices, or in password manager applications (Apps).

- Include any multi-letter word, proper nouns, or names (person, pet, or fictional character) (whether spelled forward or backward) used alone, or appended with a single-digit or with a two-digit year string, such as 98xyz123.

- Use an employee serial number, Social Security Number (SSN), birth date, phone number, remote access serial number, or information about the user that could be easily guessed.

- Enter any password or access control number (*e.g.,* PIN code) if someone is watching your keyboard.

- Share or disclose passwords.

6. DATA PROTECTION

The following ROB regarding what users must and must not do govern the USAID users' responsibility to protect the confidentiality, integrity, and availability of information.

Users must:

- Restrict disclosure of USAID information to those who have a business need and are authorized to receive the information.

- Remove your Personal Identity Verification (PIV) or Personal Identify Verification Alternative (PIV-A) card from the card reader whenever you step away from your personal computer (PC) work area to lock your PC laptop or workstation.

- Log off or lock Mac workstation, desktop, or laptop computer, or use a password-protected screensaver, when away from designated work areas.

- Completely log off when away from designated work areas for more than two hours.

- Handle all USAID information including record and non-record material in accordance with **ADS 502, The USAID Records Management Program**. USAID information must be stored on a GFE or USAID-approved network/cloud resources.

- Securely store all removable media when not in use.

- Follow established guidelines when transporting media (see **ADS 545**, **12 FAM 530**, **12 FAM 540**, **12 FAM 630**).

- Refer all external requests for access to USAID information to the Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) at **foia@usaid.gov**, in accordance with **ADS 507, Freedom of Information Act** requirements.

Users must not:

- Attempt to bypass access control measures.

- Store USAID information on personal equipment, media, or non-USAID approved network/cloud resources unless following the policy outlined in **ADS 502, The USAID Records Management Program** regarding the use of non-USAID approved equipment and media.

- Save USAID information locally (*e.g.,* to the hard drive), to GFE desktop and laptop computers unless a copy is also stored on the USAID network. Files saved locally will not be backed up by M/CIO and will not be able to be restored if the device is damaged, lost, or stolen.

- Use USAID systems for data mining unless explicitly authorized to do so by M/CIO.

7. PROTECTION OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION

The following ROB regarding what users must and must not do apply to users of information technology resources that process USAID classified or sensitive but unclassified (SBU) information, or that connect to USAID systems.

Users must:

- Protect SBU information in accordance with **12 FAM 540** and **12 FAM 544**, which includes personally identifiable information (PII) as defined in **ADS 508**.

- Mark and handle sensitive information as SBU in accordance with **12 FAM 540** and **544**.

- Mark and handle classified information, as appropriate.

- Protect SBU and classified information in all formats, including oral, paper, and electronic formats.

- Protect SBU and classified information from disclosure to unauthorized persons or groups by ensuring that only those people who have a clearly demonstrated need to know and the proper authorization (*i.e.,* a valid security clearance) of the SBU or classified information are given access.

- Contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and SEC/CTIS/IIS at (202) 712-0990 or **secinformationsecurity@usaid.gov** immediately to report any potential classified information or SBU or PII spillage incidents.

- Follow the shipping guidance contained in **ADS 508** when mailing SSNs or other PII.

- Secure paper and mobile media with SBU or PII in a locked drawer or cabinet.

- Use encryption when sending sensitive information by email (Adobe Acrobat or WinZip), regardless of whether it is sent inside or outside of USAID. This guidance also applies to .gov email accounts. See **https://pages.usaid.gov/privacy/document-encryption** for guidance on how to encrypt sensitive information.

- Check for sensitive or classified information in email strings and attachments before sending email outside of USAID approved domains, which include only usaid.gov, state.gov, ofda.gov, or oti.gov. Any classified information sent outside of Agency classified networks must be reported to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and SEC/CTIS/IIS at (202) 712-0990 or **secinformationsecurity@usaid.gov** immediately to report any potential classified information spillage incidents.

- Refer all external requests for access to SBU to M/MS/IRD at **foia@usaid.gov**, in accordance with **ADS 507, Freedom of Information Act** requirements.

- Ensure SBU on electronic media is stored in accordance with **ADS 508** and **ADS 502** requirements.

- Destroy SBU including PII in paper format by cross-cut shredding or through the use of Agency burn bags (see **ADS 568**).

Users must not:

- Participate in unacceptable use of classified information systems as referenced in **12 FAM 600**, **12 FAM 610**, **12 FAM 630**, **ADS 565**, and **ADS 568**.

- Leave SBU unattended on a printer, fax machine, or copier.

- Leave classified information unattended at any time. Classified information must be locked within a GSA-approved container (safe) when not in one's direct personal control.

- Leave SBU or classified information visible on a desk when not in one's direct control.

- Access, process, or store classified information on any USAID IT device or personal device that has not been authorized for such processing.

- Communicate or store SBU or classified information over voicemail.

- Store USAID SBU or classified information on personal equipment.

- Send and/or store USAID SBU or classified information to a personal email account.

- Store USAID SBU or classified information on cloud-based solutions not approved for Agency use by M/CIO (see **M/CIO Approved Software Portfolio**).

- Include the Social Security Number of an individual on any document sent by U.S. Mail unless it is approved by the Administrator or his/her designee.

8. INFORMATION SHARING

The following ROB regarding what users must do apply to USAID established disclosure guidelines when releasing information.

Users must:

- Confirm that the information has been shared on the Agency's external-facing public website (*e.g.,* **www.usaid.gov**) before sharing the information.

- Contact the Operating Unit that is the custodian of the information, **open@usaid.gov**, and/or **foia@usaid.gov** for guidance on if materials may be shared outside of the Agency.

- Contact **privacy@usaid.gov** if materials contain PII before sharing information outside of the Agency.

- Follow established disclosure guidelines when releasing information. Related information may be found in: **ADS 507, Freedom of Information Act**, **ADS 508, Privacy Program**, **ADS 557, Public Information**, **ADS 558, Use of Social Media for Public Engagement** , **ADS 559, Public Activity**, **ADS 560, News Releases and Services**, and **ADS 579, USAID Development Data**. If questions are not addressed in the ADS chapters, please contact the chapter points of contact.

9. INTELLECTUAL PROPERTY MANAGEMENT

The following ROB regarding what users must do are relevant to USAID requirements to protect the confidentiality and integrity of information.

Users must:

- Understand that all information processed, generated, or stored on any USAID information system has property rights and licensing requirements that must be followed. Users must ascertain and follow such rights/licenses.

- Work with GC to identify USAID's intellectual property rights for using, storing, or distributing copyrighted materials, and where necessary obtain the permission of the author/owner and use the appropriate citation to the materials.

- Contact GC for clearance before signing a Non-Disclosure Agreement (NDA), including NDAs with a third party to work with third-party intellectual property while employed by USAID.

10. AUTHORIZED AND USAID-SPONSORED SOCIAL MEDIA REPRESENTATION

The following ROB regarding what users must and must not do govern the creation and use of official USAID-sponsored social media sites or accounts, or posts in an official capacity on behalf of the Agency.

Users must:

- Understand that social media content published on official Agency social media accounts could be considered to be a Federal record, and subject to Federal record-keeping requirements and FOIA requests.

- Understand that with social media comes the ability to comment and engage directly with the public. When responding on official handles or on behalf of the Agency, USAID response to comments must be vetted and approved by the Bureau for Legislative and Public Affairs (LPA) in USAID/Washington or the Development Outreach Coordinator in Missions if relevant to individual countries, and affected Bureau/Independent Office (B/IO) leadership.

Users must not:

- Post SBU or classified information of any kind on social media.
- Post official Agency positions on social media unless explicitly authorized by LPA.
- Post, make comments, or respond to comments on social media regarding official USAID business unless you are the Agency designated spokesperson.

11. INFORMATION TECHNOLOGY INCIDENT REPORTING

The following ROB regarding what users must do govern information technology incidents.

Users must:

- Immediately report potential and actual IT security incidents to the M/CIO Service Desk by phone at (202) 712-1234 or by email at **cio-helpdesk@usaid.gov**.
- Report all potential and actual privacy breaches immediately to the M/CIO Service Desk 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.
- Contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and SEC/CTIS/IIS at (202) 712-0990 or **secinformationsecurity@usaid.gov** immediately to report any potential classified information spillage incidents.

Incident reporting standards can be found in the Privacy Breach Response and Reporting section of **ADS 508** and **ADS 545**.

12. PHYSICAL ACCESS AND ACCESS TO RESTRICTED SPACES

The following ROB regarding what users must do govern the access of USAID restricted space.

Users must:

- Protect their building access badge and other USAID access mechanisms.
- Follow restricted access procedures, including signing in and properly escorting visitors (see physical facilities and restricted spaces security procedures in **ADS 545max, Access Procedures and Guidelines for Information Technology (IT) Telecommunications (Telecom) Closets**, **ADS 562**, **ADS 565**, and **ADS 568**).

13. TELEWORKING AND REMOTE ACCESS

The following ROB regarding what users must do apply when teleworking from home or other alternate workplaces.

Users must:

- Follow security practices that are the same as, or equivalent to, those required of you at your primary workplace. These include printing securely, facing the computer screen away from windows, protecting passwords, viewing SBU information securely, etc.

- Physically protect any GFE used for teleworking, even when it is not in use.

- Prevent unauthorized disclosure of SBU.

- Protect SBU at your alternate workplace. This includes properly disposing of SBU (*e.g.,* authorized shredding) and properly securing it to prevent unauthorized disclosure (see **ADS 405.3.9 Security and Safeguarding of Government Information** for additional guidance).

- Protect SBU and PII by using only USAID-authorized removable storage media (*e.g.,* Ironkey USB flash drives), and desktop/laptop computer hard drives (or solid state equivalents thereof) encrypted using USAID authorized encryption standards.

14. PROTECTION OF COMPUTER RESOURCES

The following ROB regarding what users must and must not do apply when accessing USAID computing resources that process USAID information or connect to USAID systems.

Users must:

- Keep the laptop or mobile device under their physical control at all times, or secure it in a suitable locked container or other secure location.

- Surrender mobile devices when their safety or life is threatened.

- In AID/W report the theft to local law enforcement and contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to report the theft and submit the theft report to M/CIO in USAID/W.

- Report the theft to the Regional Security Officer (RSO) and local law enforcement if directed to by the RSO, and contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to report the theft and submit the theft report to M/CIO.

- Comply with official requests from the U.S. customs official to unlock GFE devices or to provide the official with the password to unlock the devices. Once the inspection is complete, users must change the password immediately after the device is returned.

- Understand that if GFE mobile devices are removed from your physical control at any time, including during a lawful or unlawful search, the incident must be reported to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**.

- Comply with the requirement that sensitive information processed, stored, or transmitted on wireless devices (*e.g.,* laptops, mobile phones, tablets) and laptops computers must be encrypted using Agency approved encryption methods.

- Immediately unplug mobile devices that may have been compromised from the network and notify the M/CIO Service Desk at **cio-helpdesk@usaid.gov**.

Users must not:

- Connect GFE mobile devices that were removed from their physical control including during a lawful or unlawful search until the Bureau for Management, Office of the Chief Information Officer, Information Assurance (M/CIO/IA) has approved.

- Tamper with existing encryption methods on mobile applications or any other IT resource for data at rest or in transit, or use any unauthorized encryption tools.

- Allow an infected mobile device to connect to any USAID networks (wireless or wired) or to any GFE.

- Physically connect non-GFE mobile device to the USAID networks or information systems unless it is specifically identified for guest use (*e.g.,* Guest Wireless).

- Use a mobile device to store, process, or transmit security combinations, PINs, or SBU security in unencrypted formats.

15. ACKNOWLEDGEMENT STATEMENT FOR RULES OF BEHAVIOR

I acknowledge that I have read the Rules of Behavior, that I understand the Rules of Behavior, and that I must comply with them. I understand that I am given access to only those systems and facilities for which I require access to perform my official duties. I understand that failure to comply with these rules may result in corrective measures, following due process, for Direct-Hire employees in accordance with **ADS 485**, **ADS 487**, and **ADS 568** and for Personal Services Contractors, the Federal Acquisition Regulation, and the USAID Acquisition Regulation. For contractor personnel, failure to comply may result in one or more of the following actions: verbal warnings or counseling, written warnings or counseling, revocation of privileges and/or removal from a contract supporting USAID. Where such actions may be criminal in nature, I acknowledge that the matter will be referred to the USAID Inspector General for action, including a Department of Justice Assistant U.S. Attorney.

Name of User (printed): _____

Bureau/Office/Division: _____

Physical Work Address:_____

Supervisor's Name: _____

Supervisor's Phone Number: _____

Select one:

☐ Direct Hire ☐ Personal Services Contractor ☐ Institutional Contractor ☐ Other

Contract Number *(PSCs and Institutional Contractors only)*:_____

(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):

Contractor Company Name (if applicable): _____

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 (may request the certificate of completion by emailing **IA_Training@usaid.gov**).