Acceptable Use Policy for Information Technology Resources

A Mandatory Reference for ADS Chapter 545

Full Revision Date: 05/18/2017
Responsible Office: M/CIO/IA
File Name: 545mam_051817

1. Introduction

In accordance with **ADS Chapter 545, Information Systems Security**, this document establishes USAID's acceptable use policy, as well as disciplinary actions for misuse of information technology (IT) resources. The USAID workforce must use these services in accordance with this policy. The policy outlined in this document is applicable only to unclassified devices and systems that cannot process classified information. Contact the Office of Security (SEC) for guidance on processing classified information.

2. Overview

This reference provides direction to the USAID workforce on the rules regarding use of IT resources. It applies to all personnel who perform functions on behalf of and at the direction of USAID (see applicability statement).

IT resources that are covered by this policy include:

- Official Agency email and electronic messages;
- Internet access from a USAID computer or device;
- Software installed on a USAID computer or device; and
- Government furnished equipment (GFE) such as hardware or mobile devices (e.g. phones or tablets).

All technology provided by USAID, including computer systems, communications networks, Agency-related work records, and other information stored electronically, is the property of the Agency and not the individual. Personnel do not have the right to operate USAID IT resources for personal use except on a limited basis (see section 3). This includes the personal use of GFE, such as mobile devices, inside and outside of the traditional business environment. Individuals other than the Agency workforce (e.g., family members, friends, etc.) are not authorized to use GFE.

Agency personnel should not have any expectation of privacy when using GFE (section 4). The Agency monitors online activities and data connections (section 5).

The requirement to have IT certified by USAID leadership is covered in section 6. Uses of IT resources that are deemed to be unacceptable are discussed in section 7. Misuse of IT resources can result in sanctions (section 8).

3. Who Does the Acceptable Use of IT Resources Policy Apply To?

Throughout this mandatory reference, 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, Fellows, Participating

Agency Service Agreements (PASAs), and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS 501.1**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to HSPD-12 and Information Security requirements.

4. Acceptable Limited Personal Use, Defined

Acceptable limited personal use of an IT resource means using the resource for purposes other than accomplishing official or authorized activities, but doing so in a manner that:

- Does not adversely affect one's job performance or productivity;
- Does not disrupt the work or productivity of others;
- Is of negligible cost (defined as minimal communications costs for voice, data, or video image transmission; use of consumables in limited amounts, such as paper, ink, toner; limited general wear and tear on equipment; minimal data storage on storage devices; and limited transmission impacts with moderate email message sizes, such as emails with small attachments) (see **5 CFR 2635.704(a)**);
- Is limited in duration;
- Is limited to situations in which the individual is already using Agency equipment or services (for example, an individual should not make a trip to the office for the specific purpose of using an office computer for personal business);
- Does not interfere with the mission or operations of USAID;
- Does not violate USAID policy for **ADS 545, Information Systems Security**, **ADS 508, Privacy Program**, or **ADS 545mbd, Rules of Behavior for Users**; and
- Does not violate any laws or regulations (U.S. and/or host country) (see regulations on **Standards of Ethical Conduct for Employees**).

Remember that USAID is not obligated to allow personal use of its IT resources; it does so for the convenience of its workforce. Therefore, the Agency workforce should become familiar with the guidelines in this document and use common sense before they act to ensure that they do not abuse this privilege.

5. No Expectation of Privacy

Personnel must understand that any use of USAID IT resources, including USAID government furnished equipment (GFE), email, and third party Web sites and applications (TPWAs), is not private, nor anonymous, and may be subject to disclosure

to the public under the Freedom of Information Act (FOIA). If USAID personnel wish their private activities to remain private, they should avoid making personal use of USAID IT resources. If they do decide to use USAID IT resources for personal use, personnel should not enter their own personally identifiable information (PII) when using applications or tools on these devices (for example, bank account information, address, or birthdate).

6. Agency Monitoring of Data Communications and Online Activity

The Agency may monitor electronic data communications and online activity, and disclose the collected information to Agency personnel with a need to know in the performance of their duties or to external law enforcement agencies. For example, after obtaining management approval, technical staff may employ monitoring tools in order to maximize the utilization of their resources, which may result in the detection of unacceptable usage.

7. Certification by CIO/CISO Is Required

Before a USAID Operating Unit may establish, operate, maintain or permit the use of IT on the USAID system, the USAID Chief Information Officer (CIO) or Chief Information Security Officer (CISO) must certify that it is compliant with USAID's information security policies.

Note: This applies to the use of all web-based solutions (free or others) used to conduct Agency business (e.g. any software for which USAID does not maintain an operational license).

8. Misuse and Unacceptable Use of IT Resources

USAID personnel must conduct themselves professionally in the workplace and refrain from using government furnished equipment, Internet (AIDNet and Guest Wireless), email, software, and third-party Web site applications for activities that are not related to a USAID business purpose, except for the limited personal use stated in section 3.

Specific guidance is provided below:

A. Personal use of an IT resource that could cause congestion, delay, or disruption of service to any USAID IT resource is unacceptable (for example, sending bulk emails, such as electronic greeting cards, or viewing/listening to streaming audio or video content from the Internet).

B. Do not use another person’s digital authentication, including another person’s personal identity verification (PIV) or PIV alternative (PIV-A) card.

C. The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials is prohibited. This does not apply to business partner(s) and donor Web sites that may contain

material that is used in support of federal efforts to stop human trafficking, slavery, etc.

D. It is prohibited to use USAID IT resources for activities which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities.

E. The intentional creation, downloading, viewing, storage, copying, or transmission of materials related to gambling is prohibited.

F. Do not use USAID IT resources for activities that are inappropriate or offensive to fellow personnel or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.

G. Do not physically connect personally-owned IT resources, including mobile devices such as tablets, cell phones, and media players, to existing USAID IT resources, and do not reconfigure systems. Do not modify GFE, including loading personal software or making configuration changes, without the appropriate management authorization from M/CIO.

H. Do not use USAID IT resources for commercial purposes or in support of commercial "for-profit" activities or other outside employment or business activities (such as consulting for pay, sales or administration of business transactions, and/or sales of goods or services). USAID personnel are specifically prohibited from using GFE to maintain or support a personal private business. Examples of this prohibition include personnel using a government computer to run a personal business such as an eBay "store." The ban on using GFE to support a personal private business also includes using USAID IT resources to assist relatives, friends, or other persons in such activities. Personnel may, however, make limited use of GFE under this policy to, for example, check their Thrift Savings Plan or other personal investments, to seek employment, or communicate with a volunteer charity organization.

I. Engaging in outside fundraising activities, including non-profit activities, endorsing a product or service, participating in lobbying activities, and engaging in partisan political activities, are prohibited (see **Agency Guidance on Hatch Act Requirements**).

J. Posting Agency information to external newsgroups, bulletin boards, or other public forums (to include TPWA technologies) without authority is not permitted, including information which is at odds with Agency missions or positions. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained. For questions on this matter, personnel should contact the Office of the General Counsel, Office of Ethics and Administration (GC/EA) (see **ADS 508, USAID Privacy Program**, **ADS 545,**

Information Systems Security, **ADS 565, Physical Security Programs (Domestic)**, and **ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program**).

K. USAID users must ensure that they do not give the false impression that they are acting in an official capacity when they are using USAID IT resources for non-government purposes. If there is expectation that such personal use could be interpreted to represent the Agency, then an adequate disclaimer must be used. For example: "The contents of this message are mine personally and cannot be construed to be endorsed (implicitly or explicitly) by the United States Government or by my Agency."

L. Do not establish personal, commercial, or non-profit organizational Web sites on government owned machines.

M. Do not create a Web site or TPWA on behalf of USAID without the proper official authorization.

N. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter, is prohibited.

O. The intentional unauthorized creation, downloading, viewing, storage, copying, or transmission of any controlled information is prohibited. Controlled information includes computer software and data with information that is subject to the Privacy Act, copyrighted and trademarked material, material with other intellectual property rights (beyond fair use), proprietary data, and export controlled software and data.

P. To protect privacy rights of the Agency workforce, do not use USAID IT systems or TPWA technologies to obtain or attempt to obtain information about individuals unless there is authorization to view or access the information and a legitimate business need. Do not distribute or use information about individuals unless authorized to do so.

Q. Do not use or create unauthorized automated mailing lists or distribute unauthorized newsletters.

R. USAID systems must not be used as a staging ground or platform to gain unauthorized access to other systems.

S. Sending anonymous messages other than through Department-approved surveys is prohibited.

T. Using Peer-to-Peer (P2P) file transfer technologies without Chief Information Officer (M/CIO) (or delegate) approval is prohibited.

9. Sanctions for Unacceptable Use of IT Resources

USAID B/IO/Ms, with guidance from M/CIO, may impose sanctions on individuals who use USAID IT resources for unauthorized or inappropriate purposes. Sanctions may involve administrative, disciplinary, or adverse actions, such as verbal or written warnings or counseling, revocation of privileges, and up to termination of employment. Contractors who misuse IT resources must be reported to the Contracting Officer Representative (COR). The COR must escalate misuse of IT resources to the Contracting Officer (CO), who will take appropriate action to address the situation. In extreme cases, sanctions may result in criminal penalties or financial liability on the part of the employee or contractor for the cost of the inappropriate use.

Note: When traveling on official business, personnel must contact their AMS Officer or EXO for guidance on requirements regarding purchase of local SIM cards or International Calling cards. If personnel incur unapproved fees for roaming while on official travel, the B/IO/M leadership must determine if the individual is responsible for reimbursing USAID for these unapproved expenses.

All violations of the Acceptable Use for IT Resources Policy must be reported to the M/CIO Service Desk by the employee's supervisor or the contractor's COR to initiate a review of the violation(s).

Please see **ADS 487saa, Table of Offenses and Penalties** for additional guidance on penalties for misuse of IT resources.

10. Exit Guidance

For additional guidance on requirements related to exit, please see **ADS 451, Separations and Exit Clearance**, **AID Form 451-1**, **AID Notice 03198**, and **AID Notice 01159**.

11. Questions

USAID personnel with questions about implementation of this policy should contact M/CIO at **ATO@usaid.gov**.

12. References

This policy implements requirements and guidance from the following sources:

- **5 CFR 2635.704(a)**
- Office of Management and Budget (OMB), **M-04-26, Personal Use Policies and "File Sharing" Technology**
- **ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct – Civil Service**

- **ADS 487saa, Table of Offenses and Penalties**

545mam_051717