Media Handling Procedures and Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mas_060106_cd44

Information System Security
Media Handling Procedures and Guidelines
for Users, Help Desk Staff, System Administrators and Information System Security Officers

1. Introduction

This document defines the processes and guidelines you must follow when handling media, such as tapes, memory sticks, and diskettes, used in any USAID information system.

2. Media

You can use media both to store sensitive information and to carry it from one location to another. To protect the information, you must safeguard the media against disclosure, theft, or damage. Proper media labeling, storage, transport, and disposal are risk mitigation controls.

The following sections describe how to handle different media types and events in the media lifecycle. When in doubt about the information stored on media, label, log, and securely store media.

3. New Media

You should inspect new media for damage and verify that it is in good working order before use. When you use media to store or transfer sensitive or restricted release information information, you should label and properly store the media, as outlined in **12 FAM 540**, which provides a basic Sensitive But Unclassified (SBU) definition and associated handling guidelines and **12 FAM 660** which provides communications security guidelines related to SBU information.

4. Media Storage

If you cannot control access to media during normal operational hours, the media contains sensitive or restricted release information, and you cannot physically secure your workspace or area, then you must store the media securely within a locked container, office, or suite.

5. Media Transfer

You can use media to transfer sensitive or restricted release information between devices or between individuals. Transfers may be local or remote, and you should handle them according to the following guidelines:

- **Transfer between devices**. When you use media to transfer information to another computing device, log the transfer to record the change in location. If you use a memory stick to transfer working files from your desktop to your laptop, no logging is necessary. If you use media to transfer large volumes of information/data to alternate information systems, you should log the transfer and label the media (CDROM or other permanent media).

- **Transfer within USAID control**. When you reassign media to another user, you may need to "sanitize" the media to remove any residual data before the media is given to its new "owner." For information on removing residual data from media, see the **Information System Security**

Data Remanence Procedures. You may also need to log such transfers, dependent upon the transferred information's sensitivity or the volume of information transferred.

- **Transfer outside USAID control (non-maintenance related)**. When you transfer media containing information outside USAID control for non-maintenance purposes – for example, assignment to non-USAID staff with no intention of retrieval – you must log the transfer. Following logging, you may transfer the media, either by physical hand-off or by shipping. Such media may need to be "sanitized." For information on removing residual data from media, see the **Information System Security Data Remanence Procedures.**

- **Maintenance**. When you need to send media out for maintenance or repair, you must submit the device for processing to remove any residual data **before** the device transfers from USAID control. You must also log the transfer to the maintenance vendors. You may then send the device for repair. When the device returns from maintenance, you must log that it has been returned, and either put it back into use, or store it for later use. For information on removing residual data from media, see the **Information System Security Data Remanence Procedures**.

If you need to send media instead of hand-transferring it, you must package the media in such a way that does not disclose its contents, or the sensitivity of the information contained on the device. You must label and package the media as outlined in **12 FAM 540** and **12 FAM 660**. You must send media between USAID offices and facilities by means that maintain control and accountability during transport. The recommended method is hand-transfer, but any mechanism, such as contract courier, diplomatic pouch, or commercial contract courier service, that maintains control during transport is acceptable.

6. Media Used in an Investigation

You may also encounter media that contain information required during a security investigation, such as audit trails and logs. You must maintain control of such media. You must sign it in and out in the presence of witnesses, retained as sealed, and stored where limited and logged access controls are in place.

When handling media used in an investigation, you must adhere to the following rules:

- You must not alter the media in any way.
- You must not duplicate the media unless necessary.
- You must not remove the media from storage unless authorized to do so.
- You must log the removal from, and return of media to, secure storage.
- You must retain media used in an investigation until its release is authorized by the CISO.

7. Media for Systems of Record

You must handle and store media used with USAID Systems of Record in accordance with the Record Retention Policy. This policy covers what and how long this media must be kept.

8. Restricted Media

You may release or duplicate restricted media only if authorization is given by the System Owner, ISSO or CISO to do so. You must label and properly store restricted media as outlined in **12 FAM 540**, which provides a basic Sensitive But Unclassified (SBU) definition and associated handling guidelines and **12 FAM 660** which provides communications security guidelines related to SBU information.

9. Disposal of Media (End of Life)

When media has reached its end of life, you must dispose of it securely. The following are examples of end of life conditions for media:

- It cannot be erased (e.g. permanent media, such as CD-ROMs),
- It is broken beyond repair,
- It is too costly to repair,
- It is outdated technology,
- It capacity has been exceeded,
- It has been replaced by upgraded technology, and
- It has exceeded the number of allowable times for reuse (e.g. backup tapes, cleanup tapes).

You must dispose of such media securely, using a CISO-approved method. These methods include, but are not limited to:

- Surplusing,
- Donating to charity,
- Buy back by the vendor,
- Destruction, and
- Inter-agency transfer.

Before disposing of the media, you must verify that no residual data can be extracted from the media. To do so, you may need to "sanitize" the media. For information on removing residual data from media, see the **Information System Security Data Remanence Procedures**.