Data Remanence Procedures

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mak_060106_cd44

Information System Security
Data Remanence Procedures
for Users, Help Desk Staff, System Administrators and Information System Security Officers

1. Introduction

This document defines the processes that you must follow for removing residual data from USAID media, such as tapes, memory sticks, and diskettes, and other media that contain sensitive information, when the media is disposed of or transferred from USAID control.

2. Data Remanence

Data remanence is the physical representation of data that remains after information is deleted from any device. Data remanence on media presents a risk because its presence could allow the information that was "removed" from the media to be recovered. You must overwrite or render the media unreadable to prevent the disclosure of sensitive information to unauthorized parties. You must follow data remanence procedures when media is leaving USAID control for maintenance, repair, etc., or when the media is at the end of its useful life. You also may need to follow data remanence procedures when the device is reassigned, if the information contained on the device is no longer needed by the new "owner."

Under certain circumstances, data remanence removal may not be possible or desirable (due to the sensitivity of the data, or a problem with the media). In such cases, you may request a waiver from the CISO. The CISO will either grant the waiver or provide additional guidance.

3. Data Remanence Procedure

This procedure begins with a basic question; does a condition exist that warrants the submission of a waiver to the CISO? If it does, and the waiver is granted, you do not have to follow the data remanence procedures. However, if no waiver is requested or granted, you must determine if the media can be erased using an approved erasure method as described in Section 3.1, *Erasure*, of this document. If the media cannot be erased, it must be destroyed as described in Section 3.2, *Destruction*, of this document.

There are three approved ways, divided into two categories, to remove or make data unreadable. A general description appears below. The flowchart in Section 4 describes the data remanence procedures for the local Help Desks, System Administrators, and ISSOs.

3.1 Erasure

When data is deleted from reusable media, such as a file on a floppy disk, only the pointer to the data is removed, not the data itself. The storage area that contains the file contents needs further attention to remove the actual data stored on the media.

- **Overwriting**. Software is typically used to write a pattern of ones and zeroes to storage locations, effectively overwriting data remanence. You must use CISO-approved overwriting software.

- **Degaussing**. A process whereby magnetic media is erased, also called "demagnetizing." You must use a CISO-approved degausser. It is important to note that a degausser needs periodic testing to ensure that the equipment is working properly. The recommended erasure method for magnetic tapes and floppy disks is degaussing.

For certain permanent media, such as CD-ROMs, where erasure is not possible; destruction is required.

3.2 Destruction

You can render media unreadable by physically destroying the media so that the data cannot be recovered. Destruction is generally used when media reaches the end of its useful life. Media to be destroyed should first be erased using one of the methods described above, where possible. You may use the following techniques to destroy media:

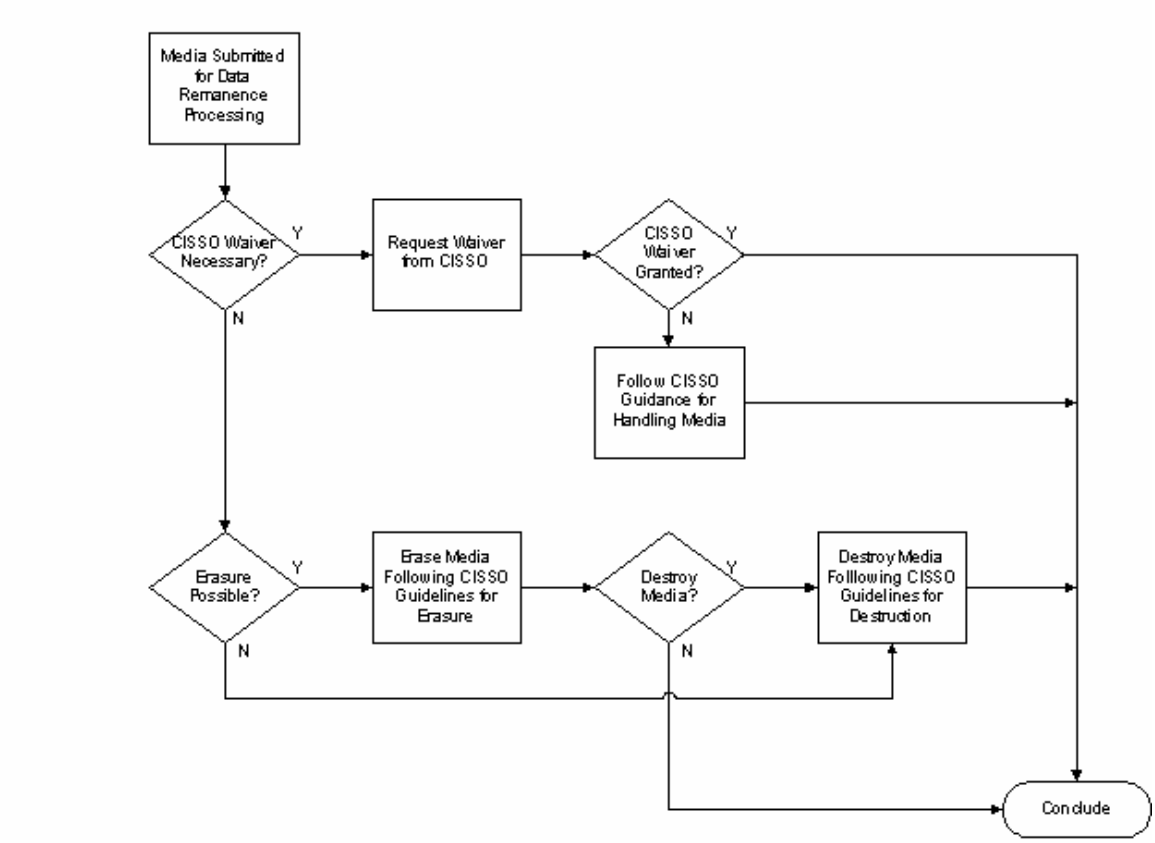
- **Pulverizing**. Media is shattered or ground into small, non-reconstructible pieces.
- **Incineration**. Media is burned in a fire until it is rendered non-usable.
- **Abrasion**. Media is destroyed using an abrasive device to rub away the recording surface.
- **Shredding**. Media is mechanically cut into small, non-reconstructible pieces.
- **Acid**. Media is destroyed using an acidic substance to burn away the recording surface.

The destruction technique you use must be CISO-approved.

4. Data Remanence Flowchart

The following flowchart describes the data remanence procedure for the local Help Desks, System Administrators, and ISSOs.

USAID Data Remanence Procedures
User, System Administrator, Help Desk and Local ISSO



The above graphic shows the decisions and steps involved in the Data Remanence Procedure as described in this document. .