OICT
Office of Information and Communications Technology

ICT Security/TPSS/SMS

version 0.8

15 December, 2009

Guideline for Information Media Sanitization[1]

The purpose of this guideline is to inform staff of available methods and tools to sanitize information media. It also aims to raise awareness of the risks related to residual data on information media and the corresponding requirement to sanitize or destroy all information media before they are reused or disposed.

In order to prevent the unauthorized disclosure sensitive information[2], such information has to be effectively removed from all information media (hard drives of servers, desktops and laptops, backup tapes, removable media such as CD's, DVD's, USB "sticks", floppy disks, ZIP disks or external hard drives, Blackberry devices, MP3 players, etc.) before the media can be reused or recycled.[3]

Sanitization types

Information media can be disposed, deleted, cleared, purged or destroyed. These terms are defined below.

Disposal is the act of discarding media with no other sanitization considerations.

Deletion of information on electronic media is a misleading term; in most cases only the references to the "deleted" data are removed, while the data themselves are still stored on the medium. "Deleted" data can therefore be often easily recovered from such media.

Clearing is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk or file recovery tools and be resistant to keystroke recovery attempts executed from standard input devices and data scavenging tools.

Purging is a media sanitization process that protects the confidentiality of information against a laboratory attack. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment.

Destruction of media is the ultimate form of sanitization. It is also the only method to sanitize write-once media such as optical disks (CD's or DVD's). After media are

---

[1] The present guideline is based on best practices, in particular the NIST Special Publication 800-88 *"Guideline for Media Sanitization"*, September 2006; and Gartner's research paper G00158207 *"Best practices for Data Destruction"*, May 2008

[2] The classification and handling of sensitive information is regulated by ST/SGB/2007/6.

[3] ST/AI/2001/4 stipulates that obsolete ICT equipment should be donated to permanent missions, other United Nations organs or non-governmental organizations.

destroyed, they cannot be reused as originally intended. Unless media can be reliably purged, destruction is the preferred method of sanitization for highly sensitive data.

Sanitization requirements

The appropriate sanitization type for electronic media depends on the sensitivity[4] of the information that had been stored on the information media as well as on the subsequent use. The cost versus benefit of a media sanitization process should also be considered prior to a final decision. Even though clearing or purging may be the recommended solution, it may be more cost effective to destroy media rather than use one of the other options.

Users and service providers should also consider the disposal of information assets at the outset, i.e. when deciding which media or system to use to store the information.

The minimum sanitization requirements are provided in the table below.

Table 1: Minimum sanitization requirements for electronic storage media

sensitivity \ subsequent use		discard/recycle (external)	reuse (internal)
Internal (see ST/SGB/2007/6)	STRICTLY CONFIDENTIAL	purge or destroy*	purge
	CONFIDENTIAL	purge	clear
	UNCLASSIFIED	clear	delete
Public		dispose	dispose

*Unless media containing information classified as STRICTLY CONFIDENTIAL are intended for internal reuse, they must be destroyed if they cannot be purged effectively.

Approved sanitization methods

The following section describes approved methods for specific sanitization types of electronic storage media.

Clearing

There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of files but may also include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Studies have show that most modern media can be effectively cleaned by one single overwrite.

Note: overwriting cannot be used for media that are damaged or not writable.

[4] On the classification of sensitive information see ST/SGB/2007/6.

There are numerous commercial tools available that can overwrite data. The following free tools are approved and recommended for magnetic hard drives:

- "Secure Erase" was developed by the Center for Magnetic Recording Research at the University of California, San Diego. It is available at no cost at http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml.
- "Darik's Boot and Nuke" is a self-contained boot disk that securely wipes the hard disks of most computers; it will automatically and completely delete the contents of any hard disk that it can detect. The tool can be downloaded from http://www.dban.org/.

Purging

For some media, clearing would not suffice for purging. However, for ATA/IDE and SATA disk drives manufactured after 2001, the terms clearing and purging have converged. USB "flash drives", i.e. USB devices without a magnetic hard drive cannot be purged by overwriting unless this functionality is implemented in hardware as is the case for certain hardware encrypted devices.

Degaussing[5] is an effective method to purge magnetic media. However, the necessary special equipment is not generally available at United Nations facilities. In addition, degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destruction

Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverization, melting and shredding. The former methods are designed to completely destroy the media and are typically carried out at an outsourced metal destruction or incineration facility.

Shredders can be used to destroy flexible media as long as the shred size of the refuse is small enough that there is reasonable assurance that the information cannot be reconstructed (see "CD's and DVD's" below).

Minimum sanitization recommendations for media containing data

The following section describes approved methods for specific sanitization types of commonly used media. Information about sanitization methods for less common media is available form the ICT Security Unit in OICT.[6]

1. ATA hard drives
   - ATA hard drives can be cleared by using approved and validated overwriting technologies/methods/tools;
   - they can be purged by using Secure Erase.
2. SCSI drives

[5] Degaussing is the process of decreasing or eliminating an unwanted magnetic field. Data is stored in magnetic media, such as hard drives, floppy disks, and magnetic tape, by orienting the magnetic moment of very small areas called magnetic domains. Degaussing leaves the domains in random patterns, thereby rendering previous data unrecoverable.

[6] The ICT Security Unit in OICT can be contacted at the email address 'OICT Security'.

- SCSI drives can be cleared by using approved and validated overwriting technologies/methods/tools;
- they can only be purged by using a degausser which is usually not available at United Nations facilities; SCSI drives that were used to store STRICTLY CONFIDENTIAL information therefore need to be physically destroyed.

3. USB removable drives with hard drives
   - USB removable drives with hard drives can be cleared by using approved and validated overwriting technologies/methods/tools;
   - they can be purged by using Secure Erase;
4. USB removable media without hard drives (a.k.a. "USB sticks")
   - USB removable drives without hard drives can be cleared by using approved and validated overwriting technologies/methods/tools;
   - however, they can only be purged if this functionality is implemented in hardware in the device itself;
5. CD's and DVD's
   - Optical disks cannot be cleared nor purged; if they contained sensitive information they must be destroyed by
     a.) removing the information bearing layers using a commercial optical disk grinding device, or
     b.) incinerating optical disk media (reduce to ash) using a licensed facility, or
     c.) using optical disk media shredders or disintegrator devices to reduce to particles that have nominal edge dimensions of five millimeters and surface area of twenty-five square millimeters.
6. Magnetic tapes
   - Magnetic tapes can be cleared by overwriting or degaussing. Overwriting should be performed on a system similar to the one that originally recorded the data; all portions of the tape should be overwritten one time with known non-sensitive signals.
   - They can only be purged by using a degausser which is usually not available at United Nations facilities; tapes that were used to store STRICTLY CONFIDENTIAL information therefore need to be physically destroyed.