Section:	Information Security	Effective:	March 2007
Standard:	Media Control Security	Revised:	
Policy Ref:	5.8.22	Responsibility:	Chief Information Security Officer

MEDIA CONTROL (DATA DESTRUCTION) SECURITY STANDARD

Security Standards: are <u>mandatory</u> security rules applicable to the defined scope with respect to the subject.

Overview

According to Texas Government Code §2175.128, DISPOSITION OF DATA PROCESSING EQUIPMENT, State agencies must dispose of data processing equipment (i.e., computers and peripherals) in a specific manner after exhausting all transfer opportunities within the agency itself. Equipment not transferred locally (within the agency) must be offered to a local school district, to an assistance organization specified by the school district, or to the Texas Department of Criminal Justice. These agencies will have the opportunity to repair, train with, or salvage parts from the proffered equipment. To prevent data or applications on the equipment from being compromised, the Texas Department of Information Resources (DIR) requires all donated storage media be wiped of ALL data to a degree such that the data is unrecoverable. If the data cannot be destroyed with sufficient confidence, DIR requires the media be removed and destroyed prior to transfer or disposal. See HOP 6.3.3, Deletion of State Property, for references to forms and procedures for properly turning in University information resources.

Scope

All personnel responsible for managing DEPARTMENTAL data processing equipment, especially those responsible for transferring or disposing of that equipment. The responsibility for meeting this standard is at the departmental level and not with the Warehouse, General Services, or Property Control.

Purpose

The purpose of this document is to ensure all data is removed from any media before the media and system are transferred to another department or disposed of outside the University to prevent violation of software license agreements, unauthorized release of confidential information, and/or unauthorized disclosure of trade secrets, copyrights, and other intellectual property.

Structure

This standards document only represents the requirements and the specific standard. Guidelines for meeting this standard may be found at the Information Security web site (<u>http://infosec.uthscsa.edu</u>).

Special Notice

In all cases, wiping and/or physical destruction, those records subject to retention requirements according to HOP 2.2.1, Records and Information Management Retention, must be copied to an alternative storage device and must be accessible and retrievable for the duration of the mandated retention period.

Instructions

NOTE: See the associated guideline for this standard at the Information Security web site, http://infosec.uthscsa.edu, for the approved tools and processes for achieving this standard's goals and requirements, along with recommended forms and labels.

When storage media are no longer operational, or no longer needed and have been properly backed up, departments should establish a local procedure with a specific timeframe for storage of the obsolete media. Media should be locally stored for the minimum time possible to reduce the threat to the data caused by loss, theft, or accidental transfer to another agency. 30 days should be considered the maximum time before the media is wiped or destroyed. For destruction, once the media has been removed from the system to be turned in and the decision has been made to destroy the media, a label should be affixed with the date of removal and the final date for the destruction of the media.

The focus of the rest of this document is the secure removal (wiping or destruction) of data from data storage media before transfer or disposal of the associated equipment. These same standards may also be applied to clearing media for reuse within the same department.

For the purposes of this standard, references to media or storage media include, but are not limited to:

- Hard disk drives (both inside computers and external drives)
- Diskettes (floppies or floppy disks)
- Optical devices (CDs, DVDs, MOs)
- Solid state devices (flash media, USB or "thumb" drives, etc.)
- PDA and Cell Phone

To prevent inadvertent disclosure of information and/or violation of software license agreements, **all** data must be removed from the media, and, if necessary, stored properly (see **Special Notice**).

Clearing/Wiping:

Once the data is removed, the media itself must be wiped with an approved technique or tool. Regardless of technique or tool, the media must be overwritten to the following standard according to disposition of the equipment:

- Reuse within the department: single overwrite
- Transfer within the University: at least two overwrites
- Transfer outside the University: three or more overwrites

An overwrite is writing a single character or pattern of characters to every sector of the media, effectively replacing or "overwriting" the original data. For additional guidance concerning reuse or transfer within the University (repurposing), see HOP 5.8.22.

See the associated guideline (see **Structure**) for approved tools and processes.

Destruction:

If the information on the media is critical enough that disclosure MUST be prevented at all costs and wiping is not sufficient, the media must be removed and the data physically destroyed by:

- Degaussing hard disk drives at a level of 4000 Gauss or more
- Physically destroying all media

See the associated guideline (see **Structure**) for approved tools and processes.

Exceptions

Exceptions to this standard are not applicable since the direction for clearing the data comes from the State of Texas and the direction for protecting the data is driven by multiple Federal requirements, including, but not limited to, HIPAA, GLB, FERPA, etc.