Media Sanitation Guideline

This guideline defines controls for the proper disposal of all Florida International University sensitive information, either in paper or electronic format.

In order to protect University data, especially Highly Sensitive Data, from inadvertent or unauthorized use or disclosure, a University department or unit disposing of equipment with storage devices must ensure that the storage devices are erased using a repeated overwrite operation, purged, degaussied, or destroyed prior to storage media being sent to surplus, reused, donated, or discarded.

Storage media may be sanitized using several methods:

- Data Overwriting Applications
- Magnetic Degaussing
- Physical Destruction

Upon completion of media sanitation procedures, the equipment must display an official sticker from the Information Security Office indicating the name of the person who performed the cleaning, the date of compliance, and the MSCID.

Reason for Guideline

Although a large portion of University data is shared with the public, some data is restricted from unauthorized access, use or disclosure by the privacy protections mandated by state and federal laws. To comply with these mandates and to protect the University Community, the University must have procedures in place to protect, manage, secure, and control data under its purview.

This policy addresses the privacy, security, and confidentiality of University data, especially Highly Sensitive Data, and the responsibilities of institutional units and individuals for sanitation of equipment prior to its removal or disposal.

Related Information

Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. § 1232g
Florida Administrative Code 6C8-11.003 (Access to Student Education Records)
Florida Statutes §1002.21 (Postsecondary student and parent rights), §1002.22 (Student records and reports), §1006.52 (Student Records)
Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191
HIPAA Security Standards, 42 CFR §164.312
University IT Policy: Gramm-Leach-Bliley Act: Safeguards to Protect Confidential Financial Information
University IT Policy: Information Technology Security

Definitions:

Data Overwriting - Overwriting is a process of permanently and irreversibly removing or destroying the data stored on a device. In general, it writes over the previous data, hence the name. These algorithms use a precise set of rules to remove any part of an original data from the memory by writing a new raw data on the memory.
**Highly Sensitive Data** - Highly Sensitive Data is defined as information which must be protected from disclosure by state or federal law, or by binding contractual arrangement. Among the types of data included in this category are individually identifiable financial or health information, social security numbers, credit card information, student education records and proprietary data protected by law or agreement.

**Magnetic Degaussing** - Data is stored in magnetic media, such as hard drives, CD, DVD, floppy disks and magnetic tape, by making very small areas called magnetic domains change their magnetic alignment to be in the direction of an applied magnetic field. Degaussing, commonly called erasure, leaves the domains in random patterns with no preference to orientation, thereby rendering previous data unrecoverable.

**MSCID Number** - A unique identification number which is assigned to a media storage device by the Information Security Office once the sanitation process has been completed.

**University Data** - Any data created or maintained by the University in order to conduct its business operations.

**Procedures**

**Disposal of Hardcopy Records**

**Hardcopy Disposal** - When disposed of, all sensitive information in hardcopy form must be either shredded or incinerated. To ensure that documents are properly destroyed, only cross-cut or micro-cut shredders will be used to shred hardcopy records containing sensitive information.

**Secure Information Containers** – Sensitive information that is no longer needed must be placed in a designated locked container within Florida International University offices and never placed in trash bins, recycle bins, or other publicly-accessible locations.

**Litigation Hold**

**Destroying Documents Relevant To Litigation** - If there is credible reason to believe that certain Florida International University internal documents may be needed as evidence in upcoming litigation, these documents must not be destroyed by the ongoing Florida International University document destruction process. They must instead be brought to the attention of internal legal counsel and then properly secured.

**Disposal of Electronic Media**

**Storage Media Destruction** - Destruction of sensitive information captured on computer storage media must only be performed by the Information Security Department.

**Disposal of Computer Equipment**

**Used Component Equipment Release** - Before disposal, donation, or recycling, the Information Security Department must validate that sensitive information has been removed from any information systems equipment that has been used for Florida International University business. This validation process must take place before releasing such equipment to a third party.
Information And Equipment Disposal - Department managers are responsible for the disposal of surplus property no longer needed for business activities in accordance with procedures established by the Information Security Office, including the irreversible removal of sensitive information and licensed software.

Inventory Of Decommissioned Computer And Network Equipment - Information Security Office must maintain an inventory of all Florida International University computer and network equipment that has been taken out of commission.

Labeling Required - Equipment designated for surplus or other re-use should have a label affixed stating that the hard drive has been properly sanitized.

Transfer of Hard Drives and Media

Transfer of Hard Drives - Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access the data by ordinary means. All electronic media should be sanitized according to Florida International University procedures.

Transfer of Electronic Media - Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.

Attempted Recovery – Attempts to recover deleted or sanitized data must only be done by specially trained personnel approved by Florida International University management. Insofar as special recovery tools would have to be used by an individual to access the data erased by this method, any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the Florida International University Confidentiality Statement.

All academic and administrative departments and offices at Florida International University including all student organizations are responsible for compliance with the FIU Media Sanitation and Property Control guidelines, as well as University policies and procedures and applicable state and federal laws. See Property Accounting’s Surplus, Asset Transfer and Cannibalization Request Forms located at http://finance.fiu.edu/controller/forms.html.

Responsibilities:

Division of Information Technology
The Division of Information Technology through the Information Security Office will be responsible for performance and documentation of all media sanitation.

Facilities Department
It is the responsibility of the Facilities Department through the Surplus Department to ensure that no media that has been submitted for surplus, disposal or donation is permitted to be transferred to another department or leave university property without proper sanitation of storage media. The Facilities Department must ensure that all equipment that is submitted for surplus, disposal or donation bears the compliance sticker indicating that media sanitation procedures have been completed and MCSID number has been assigned.