University Community (faculty, staff and students) and Authorized Users of University’s IT Resources (e.g., consultants, vendors, visitors, contractors, etc.)

PROCEDURE STATEMENT (R)
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, degaussed, 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 IT Security indicating the name of the person who performed the cleaning, the date of compliance, and the MSCID

REASON FOR PROCEDURE (O*)
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 protect the University Community, the University must have procedures in place to protect, manage, secure, and control data under its purview.

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

RELATED INFORMATION (O*)
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
**CONTACTS (R)**

<table>
<thead>
<tr>
<th>Administrative Office’s Address</th>
<th>Telephone Number</th>
<th>Fax Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cheryl Lyn Granto</td>
<td>(305) 919-4299</td>
<td>(305) 919-5245</td>
</tr>
<tr>
<td>IT Security Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Florida International University</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11200 S.W. Eighth Street, LIB 328</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami, Florida 33199</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DEFINITION (R)**

*Data Overwriting:* Overwriting is a process of writing a binary set of data on a memory. 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 IT 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.

**RESPONSIBILITIES (O)**

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 Surplus, Transfer and Cannibalization Forms link below.

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

Facilities
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.

**FORMS/ONLINE PROCESSES (O)**

Surplus, Transfer and Cannibalization Forms http://finance.fiu.edu/controller/forms.html

*R = Required  *O = Optional