Electronic Media Sanitization Process

- Department: Information Security Management and Compliance
- Issue Date: March 2010
- Revision Date: March 2015
- Expiration Date: N/A
- References:
  - Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act)
  - California Code of Regulations, Title 22, Division 4.5, Sections 66273 & 66273.6
  - CSULB Records Management Standard
- Web Links:
  - Information Technology Services
  - Information Security Management and Compliance

I. PURPOSE

The purpose of the Electronic Media Sanitization Process document is to guide campus staff and information technology coordinators through the use of CSULB’s standardized tool and processes to securely sanitize hard disks of computers that are being:

- Surveyed for public auction;
- Disposed of (e.g. drive is too small, or no longer needed);
- Reassigned to other individuals on campus; or
- Transferred to another department on campus.

This is necessary to reduce the possibility of inappropriate exposure of data and unauthorized use.

II. SCOPE

This process applies to all University and Auxiliaries. Individual departments shall be fully responsible for ensuring storage media (e.g. hard drives) have been sanitized or destroyed prior to asset disposition or internal reassignment.

III. BACKGROUND

To protect the confidentiality of information and the related privacy rights of CSULB students, faculty, staff, donors, patrons, vendors, and others, University and Auxiliary employees, in conjunction with their Information Technology Coordinator, must ensure that electronic data in their possession is secure at all times.

When electronic computing devices and/or electronic storage media are transferred between departments or divisions, or removed from service, all electronic data must be properly sanitized prior to release of custody. The sanitization process ensures that recovery of information is not possible and that campus information security objectives are not compromised. Several methods can be used to sanitize media; however, the two major types of sanitization are clearing and destroying.

Clearing

Clearing information is a level of media sanitization that protects the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities and must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. Overwriting is an acceptable method for clearing media. The security goal of overwriting is to replace written data with random data.
There are several overwriting software products to overwrite storage space on media. CSULB Information Technology Services provides software tools and instructions to securely clean the data from electronic storage media. Overwriting cannot be used for media that are damaged or not rewritable. In such cases, electronic media should be destroyed.

**Destroying**

- When electronic media is inoperable and cannot be cleared, the electronic media must be physically destroyed. While physical destruction can be accomplished using a variety of methods, the campus has purchased a degausser for destruction of hard drives and a shredder for the destruction of other electronic media.

**IV. TRANSFERRING, SURVEYING, OR DESTROYING ELECTRONIC DEVICES AND MEDIA**

When electronic computing devices or electronic storage media are to be transferred or surveyed, area Information Technology Coordinators will work with appropriate supervisors to complete the following steps:

1. All electronic computing devices or electronic storage media must be overwritten using university-approved and validated overwriting technologies/methods/tools without exception:
   - Darik’s Boot and Nuke (DBAN) [http://dban.sourceforge.net](http://dban.sourceforge.net) (One pass is sufficient.)
2. Only instances involving an inoperable hard drive that cannot be cleared will require its’ removal from the electronic computing device in order to ensure proper destruction. Inoperable electronic computing devices and/or electronic storage media must be isolated and secured until properly destroyed. These devices will be destroyed using the degausser. Please learn about the Degausse & Destroy Media Sanitization Service provided by Information Technology Services (ITS)
3. The designated Information Technology Coordinator must complete and sign a Media Sanitization Certification form for the item(s) to be transferred or surveyed.
4. The Media Sanitization Certification must be submitted with either a Property Transfer Request Form or Property Survey Request Form to Property Management for processing.
5. Upon approval from Property Management, the item(s) may then be transferred to the new Department or Division, or surveyed to Property Management.

**V. DEFINITIONS**

**Electronic Computing Devices**

Include, but not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smart phones.

**Electronic Storage Media**

Include, but not limited to, floppy disks, ZIP disks, DVDs, CDs, external hard drives, and USB storage devices.

**Information Technology Coordinators**

University and Auxiliary employees who are responsible for maintaining electronic computing devices and/or electronic storage media for their designated areas.

**FURTHER INFORMATION**

Information Security Management and Compliance

iso@csulb.edu

(562) 985-4862

Or contact your area’s designated Information Technology Coordinator.