



# CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: <b>Media Sanitization Standard</b>	
Department: <b>Information Security Management and Compliance</b>	Reference No.:
Division: <b>Administration and Finance</b>	Issue Date: <b>August 2006</b>
References: <ul style="list-style-type: none"> <li>• <b>Fair and Accurate Credit Transactions Act of 2003 (FACTA);</b></li> <li>• <b>FCRA, 15 U.S.C. 1681 et seq.</b></li> <li>• <b>California Civil Code §1798.81</b></li> </ul>	Revision Date: <b>October 2007</b>
Web Links: • <a href="http://daf.csulb.edu/offices/vp/information_security">http://daf.csulb.edu/offices/vp/information_security</a>	Expiration Date: <b>N/A</b>

## I. BACKGROUND

The Fair and Accurate Credit Transaction Act of 2003 contains several provisions designed to help reduce the incidence of identify theft, and help victims recover their credit reputations after they have been victims of identity theft. California Civil Code Section 1798.81 requires businesses, when disposing of customer records, to take all reasonable steps to destroy personal information in the records by shredding, erasing, or otherwise modifying the personal information so that it is unreadable or undecipherable.

This Standard addresses the provisions of FACTA and California Civil Code Section 1798.81 requiring that reasonable measures be taken when disposing of any record, in any format, containing confidential information to protect against the unauthorized access to it.

## II. STANDARD

To protect the confidentiality of information and the related privacy rights of CSULB students, faculty and staff concerning this information, all software and/or files from computers, and storage devices must be sanitized prior to disposal.

The sanitization process shall remove all information from media such that data recovery is not possible. 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 it 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 replaces written data with random data.

There are several overwriting software products to overwrite storage space on the media. Network Services provide software tools and procedures to securely clean the data from ATA based hard drives and other storage media. Software and instructions are available for all campus users. Please contact the Director of Network Services at (562) 985-4750 for more information.

Overwriting cannot be used for media that are damaged or not rewriteable. In such cases, media should be destroyed.

- Destroying - Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, with cross-cut shredding being the most common practice. Departments may shred media on site or contact Procurement and Support Services for a listing of approved vendors that meet the campus **Third Party Agreements/Confidential Information Standard**.

Specific recommendations for sanitizing different media types are included in **Attachment A**.

#### **FURTHER INFORMATION**

Information Security Management and Compliance  
iso@csulb.edu.  
(562) 985-2283

**Attachment A  
Media Sanitization Methods**

<b>Media Type</b>	<b>Method</b>
<b>Hard Copy Storages</b>	
Paper	Destroy.
Microforms	Destroy.
<b>Hand-Held Devices</b>	
Cell Phones	Manually delete all information, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings.
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state.
<b>Equipment</b>	
Copy Machines	Perform a full manufacturer's reset to reset the copy machine back to its factory default settings
Fax Machines	Perform a full manufacturer's reset to reset the fax machine back to its factory default settings
<b>Magnetic Disks</b>	
Floppies	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
IDE Hard Drives	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Serial ATA Drives	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Zip Disks	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
SCSI Drives	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Reel and Cassette Format Magnetic Tapes	<p>Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.</p> <p>Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known nonsensitive signals.</p>

**Attachment A  
Media Sanitization Methods**

<b>Media Type</b>	<b>Method</b>
<b>Optical Disks</b>	
CDs	Destroy.
DVDs	Destroy.
<b>Memory</b>	
Compact Flash Drives or USB/Memory Sticks	Overwrite media by using university approved and validated overwriting technologies/methods/tools.
Other Memory Devices	Contact your area computer technician or the campus Assistant Information Security Officer at 985-4862 for the best method of sanitization.
<b>Magnetic Cards</b>	
Flash Cards	Perform a full chip purge as per manufacturer's data sheets.
Magnetic Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Personal Computer Memory Card International Association (PCMCIA) Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Smart Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
RFID	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
<b>Items Not Listed Above</b>	
Unlisted Technologies	For electronic technologies not listed in the above table, please contact the campus Assistant Information Security Officer at 985-4862.

For further information or assistance, contact your designated computer technician or the campus Assistant Information Security Officer at 985-4862.