User Guidelines for the Safe Disposal, Transfer, or Reassignment of Electronic Storage Media	Guidelines No.	ITS-1017-G	Rev:	A
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	2-3-11	Effective:	2-3-11
				Page 1 of 10

Table of Contents

1 Purpose 2
2 Entities Affected by These Guidelines 2
3 Definitions 3
4 Guidelines 5
4.1 Electronic Storage Media Sanitization and Destruction 5
4.2 When is Sanitization Warranted? 6
5 Contacts 7
6 Applicable Federal and State Laws and Regulations 8
7 Related Documents 9

1 Purpose

Computers and other forms of electronic storage media are often reassigned to another employee within a department, transferred to another campus department or division, or disposed or donated at the end of its useful life. Sometimes this equipment contains protected data, such as confidential, personal, medical, health insurance, or proprietary information, that should not be seen or used by others. It's imperative that this protected data be removed from the equipment prior to the reallocation or disposal. In addition, operating system and application software must be removed prior to donation or disposal in order for the University to remain compliant with software licensing agreements.

This document presents the guidelines to follow to ensure that protected data is permanently removed from a personal computer, workstation, server, PDA or portable electronic storage media in such a way that the data is deliberately made non-recoverable. Additionally, this document discusses when to sanitize disks and devices that may contain protected data.

2 Entities Affected by These Guidelines

All University employees using any University-owned or –issued memory device are responsible for notifying ITS or their appropriate Information Technology Consultant (ITC) before:

- Relocating, reassigning, donating, or disposing of any memory device that contains protected data;
- Returning defective memory devices under warranty to the manufacturer for replacement;
- Sending defective memory devices to a vendor or computer store for repair or data recovery.

  NOTE: These guidelines are intended to ensure memory devices are donated or disposed of safely. All employees must still adhere to all existing University policies and procedures related to equipment donation or disposal.

The responsibilities of these guidelines apply to all department administrators who must ensure that data sanitization has occurred prior to the relocation, reassignment, donation, or disposition of electronic storage media.

The technical aspects of these guidelines apply to all ITS Baseline Services personnel and campus Information Technology Consultants (ITCs) who are responsible for ensuring that memory devices are sanitized according to instructions outlined in ITS-1021-G User Guidelines for Data Sanitization.

These guidelines apply to all computer systems issued to campus users through Baseline and all IT systems that store protected data on personal computers or attached storage devices. Personal computers include portable systems, desktops, and workstations. The system user or their ITC is responsible for making appropriate backups before releasing any equipment to ITS or the ITC for data sanitization.

3 Definitions

a) Confidential Information: In addition to the personal information listed below, examples of confidential information include the following: financial records, student educational records, physical description, home address, home phone number, grades, ethnicity, gender, employment history, performance evaluations, disciplinary action plans, or NCAA standings. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.

A student may exercise the option to consider directory information, which is normally considered public information, as confidential per the Family Educational Records Privacy Act (FERPA). Directory information includes the student's: name, address, phone, dates of attendance, degrees received, major program, height and weight (if an athlete), e-mail address, enrollment status, campus, school, college, division, class standing, and awards.

b) Data Sanitization: The process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data and even advanced forensic tools should not ever be able to recover sanitized data.

c) Disposition: A range of processes associated with implementing records/information retention, destruction, or transfer decisions that are documented in the records/information retention and disposition schedule or other authority.

d) Electronic Storage Media: Electronic or optical data storage media or devices that include, but are not limited to, the following: computer hard drives, magnetic disks, CDs, DVDs, flash drives, memory sticks, tapes and Personal Digital Assistants (PDAs – e.g., Palm Pilots, Pocket PCs, and Smart phones). Also called memory devices.

e) Health Insurance Information: An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

f) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential data is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared, or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

g) Level 2 Internal Use Data: Internal use information is data that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

h) Memory Device: Devices that include, but are not limited to computer hard drives, magnetic disks, computer tapes, flash memory devices, CDs and DVDs, PDAs (Palm Pilots, Pocket PCs, and Smart phones), Zip disks, USB storage devices (flash drives, iPods, portable hard drives).

i) Personal Information: California Civil Code 1798.29 defines personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security Number
- Driver's license or California Identification Card number
- Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information

j) Portable Electronic Storage Media: Includes, but not limited to, the following: CDs, CDRWs, DVDs, Zip disks, flash drives, floppy disks, i-Pods, digital media players, and portable hard drives.

k) Proprietary Information: Information that an individual or entity possesses, owns, or for which there are exclusive rights. Examples include: faculty research, copyrighted materials, white papers, research papers, business continuity and other business operating plans, e-mail messages, vitae, letters, confidential business documents, organization charts or rosters, detailed building drawings, and network architecture diagrams. Proprietary information, if lost or stolen, could compromise, disclose, or interrupt operations or embarrass the individual or the University.

l) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance, or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

m) Record: "Authentic official copy of a document deposited with a legally designated officer…" (Merriam-Webster Online: http://www.merriam-webster.com/). Records can be in any format (handwritten, printed, digital, etc.) and can be stored on paper, computer media, e-mail, hand-held peripherals, CDs, DVDs, wireless devices, video or audio tapes, films, microfilm, microfiche, or any other media.

n) Shredder: A device that renders documents completely unreadable by slicing/mincing paper into fine pieces. Approved shredders should be NSA Level 5 compatible.

4 Guidelines

ITS and ITCs are solely responsible for:

- Performing the data sanitization process on University-owned or –issued computers and electronic storage media.
- Signing the *Electronic Data Sanitization Verification* form.
- Submitting the signed copy to Property Management (for donations or disposal) or the requesting department (for reassignments and relocations), as appropriate.

It is important to recognize that almost all operating system (OS) commands designed to delete data or format disks do not remove all the data. Such commands are only to free up the space that the deleted files consumed. Most of the actual file data remains on the disk or memory device and there are a number of forensics products that can recover these data. Therefore, unless vendor supplied operating system commands and utilities have been specifically designed to sanitize data, they should not be used for this purpose. OS commands and utilities that are capable of sanitizing data files or entire disks typically have names like “secure erase”, “secure delete” or “secure empty trash”. Options for these programs and utilities often allow a user to specify how many times the disk or data should be wiped (erased and rewritten). Not all OS vendors supply programs are capable of data sanitization. Some newer machines have standard data sanitization programs (e.g., the HP Disk Sanitizer included in the BIOS, which meets the Department of Defense (DOD) data sanitization standard).

Removing an unsanitized hard drive prior to transferring, donating, or disposing of the computer or electronic storage device is <u>not</u> an acceptable practice. Hard drives are University property and as such, must follow the same procedures for equipment disposal. In addition, these hard drives can easily be lost, forgotten, or stolen, and the protected data could then be obtained by unauthorized individuals. If the hard drive is to be removed and replaced with a new one, the original hard drive must be sanitized prior to removal and storage. Alternatively, if the department is retaining the hard drive as an archival of important department files, all files and documents containing protected data must be encrypted.

All campus users should take appropriate measures to safeguard protected data on their systems. This document also serves as a reference for individual departments to adopt a standard data sanitization process.

4.1 Electronic Storage Media Sanitization and Destruction

There is no way to use any operating system to effectively sanitize the same operating system disk. In other words, an operating system cannot securely erase the disk that it is “running off of”. One quasi-exception is that Macintosh systems may be booted from the OS installation CD or DVD, and then the Disk Utility application may be used to sanitize any attached disks. For detailed instructions on data sanitization for Apple Mac systems, refer to ITS-1021-G User Guidelines for Data Sanitization. For other operating systems, the means to securely remove protected data from disks can either be magnetic or physical destruction, or the use of specialized software utilities that make data unrecoverable. The method used will depend on the circumstances (i.e., transfer of custody, survey of assets, etc.). Magnetic destruction involves applying a strong magnetic field to the device that erases all data. Physical destruction involves drilling holes into the platters and controller cards. If a department has access to specialized tools, a more thorough approach can be taken such as either taking apart the disk and cutting the platters into small pieces or otherwise destroying the disk

(e.g., incineration or crushing). Sanitization guidelines for specific types of devices are described in the following sections:

a) **Optical Media Destruction:** CDs and DVDs that contain protected data need to be physically destroyed when they are no longer needed. Larger paper shredders can often do this, as can special CD/DVD destruction hardware.

b) **Removable Storage Devices Destruction:** Removable storage devices that contain protected data need to be physically or magnetically destroyed when they are no longer needed. Most USB removable storage devices can be sanitized with sanitization tools such as Darik's Boot & Nuke (or similar products) or by physical destruction of the device.

c) **PDA and Smart Phone Sanitization and Destruction:** Vendor software is not guaranteed to actually sanitize the memory in these devices and third-party products are more focused on encryption. It is difficult to be certain that a device has been securely sanitized. The recommended approach is to manually delete all stored information and then perform a manufacturer's hard reset to reset the device to factory state.

4.2 When is Sanitization Warranted?

The following scenarios are intended to cover all possible circumstances that would require data sanitization. In all cases, the device is assumed to contain protected data and physical custody of the device is transferred.

a) **Custody of the Device is Transferred Within a College or Division:** In this case, a device is transferred from one person to another who works in the same college / division and the new custodian has the same level of access to protected data. If the original device owner and the new owner have the same rights to view the protected data stored on the device, and there is written approval for the transfer from management, there is no need for data sanitization. The device may be transferred without removing any protected data. However, if the recipient is restricted from accessing the stored data, the files containing this data must be sanitized according to ITS-1021-G User Guidelines for Data Sanitization.

b) **Custody of the Device is Transferred to a Different College or Division:** When a device is transferred from one person to another in a different college / division, all protected data on the device needs to be sanitized according to ITS-1021-G User Guidelines for Data Sanitization.

c) **The Device is Transferred for Disposal or is Transferred Off Campus:** When a device is to be disposed of or transferred off campus, all data should be sanitized, whether or not it is known to contain any confidential data. In addition, the operating system and all software applications must be removed to ensure the campus remains compliant with software vendor licensing agreements. No system should leave the campus premises without all storage devices being either sanitized or removed.

   As part of the asset survey process, functional devices that are being disposed of are required to go through a physical destruction process as specified in ITS-1021-G User Guidelines for Data Sanitization.

d) **The Device is Defective:** When a defective device is to be sent off campus for data recovery, the vendor must comply with all information security requirements for Third Party Service Providers and agree to sign the Third Party Vendor/Consultant Information Confidentiality/Non-Disclosure Agreement (NDA), available at http://www.calstatela.edu/its/forms/ITS-2808_InfoConfidentialityNDAAgrmt.doc or provide a signed vendor NDA that meets the requirements of the CSULA NDA. Approval from the Director of IT Security and Compliance must be obtained before the transfer occurs.

> Note: The University has previously used Kroll Ontrack Data Recovery Inc., a worldwide company that has over 30 years experience in recovering lost or damaged data from computers, servers, and systems. They provide a comprehensive Non-Disclosure Agreement to hold confidential any and all data contained on the device they are servicing. Their Web site is located at http://www.ontrackdatarecovery.com.

As part of the asset survey process, defective devices that are being disposed of are required to go through a physical destruction process as specified in ITS-1021-G User Guidelines for Data Sanitization.

e) **Devices not Managed by ITS:** It is expected that custodians of systems that are not managed by Baseline and ITS will consult with their assigned Information Technology Consultant (ITC) regarding the proper sanitization procedure. Individual custodians of such devices are responsible for ensuring that all devices turned in for recycling or transfer to a third party are properly sanitized and/or destroyed before the device leaves the campus.

5 Contacts

a. For questions regarding specific department data sanitization procedures, contact the department administrator or Information Technology Consultant (ITC).

b. For assistance in data sanitization, contact the ITS Help Desk at 3-6170.

c. For assistance in encrypting files, contact your department's Information Technology Consultant (ITC).

d. For a list of Academic Affairs ITCs, visit http://www.calstatela.edu/itc.

e. For a list of Administration and Finance ITCs, visit http://www.calstatela.edu/univ/bussys/staff.php.

f. For questions regarding these guidelines or information security, contact IT Security and Compliance at itsecurity@calstatela.edu.

g. Information about FERPA requirements is available online at http://www.calstatela.edu/ferpa.

6 Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html A federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act 15 USC, Subchapter 1, Sec. 6801-6809	**Gramm Leach Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	**Standards for Privacy of Individually Identifiable Health Information** http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/guidanceallsections.pdf A federal law that protects the privacy of health records.
State	**Title**
SB 1386	**California Personal Information Privacy Act, SB 1386** http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Section 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
California Civil Code Sections 1798.80-1798.81	**California Civil Code – Section 1798.80 – 1798.81 Destruction of Customer Records** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that identifies steps to be taken in the destruction of customer's records.
Government Code Sections 14740-14769	**State Records Management Act** http://www.leginfo.ca.gov/.html/gov_table_of_contents.html Information on the administration of state records.

7 Related Documents

ID/Control #	Title
CSULA Administrative Procedure 509	**Property Survey** http://www.calstatela.edu/univ/admfin/procedures/509.pdf Establishes the policy and procedures governing the accountability, control, inventory, movement, and other responsibilities for University property surveys.
CSULA Administrative Procedure 507	**Property Control** http://www.calstatela.edu/univ/admfin/procedures/507.pdf Establishes the policy and procedures governing the accountability, control, inventory, movement, and other responsibilities for University property.
CSULA Administrative Procedure 707	**Record Retention and Disposition** http://www.calstatela.edu/univ/admfin/procedures/707/707.pdf This document establishes procedures for the transfer of University records to the State Records Center, the retrieval of stored records, and the destruction of obsolete records.
CSU Information Security Policy	**The California State University System-wide Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.
ITS-1005-G	**User Guidelines for Portable Electronic Storage Media** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1005-G_PortableElectronicStorageMedia.pdf These guidelines are intended to help students, faculty, and staff meet the University's accepted standards for protecting confidential information that is copied, downloaded, or stored on portable electronic storage media.
ITS-1021-G	**User Guidelines for Data Sanitization** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1021-G_DataSanitization.pdf These guidelines define the appropriate data sanitization tools and procedures to meet security standards.
ITS-8830	**Electronic Data Sanitization Verification** http://www.calstatela.edu/its/forms/ITS-8830_Electronic Data Disposal Verfication.doc

ID/Control #	Title
	This form must be completed to authenticate the data sanitization process for every electronic storage device prior to relocation, reassignment, donation, or disposition.
CSULA Gramm-Leach-Bliley Information Security Program	**Gramm-Leach-Bliley Information Security Program for CSULA** http://www.calstatela.edu/its/itsecurity/programs/glba.php The GLB Information Security Plan for CSULA. It serves as a guide for how information security is to be maintained at the campus.