User Guidelines for Data Sanitization	Guidelines No.	ITS-1021-G	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
				Page 1 of 12

Table of Contents

1 Purpose

Data sanitization is the process of deliberately, permanently, irreversibly removing or destroying the data stored on a memory device. These memory devices include, but are not limited to, the following: computer hard drives, magnetic disks, flash memory devices, CDs and DVDs, PDAs (e.g., Palm Pilots, Pocket PCs and Smart phones), Zip disks; and USB storage devices (e.g., flash drives, iPods, and portable hard drives). A device that has been sanitized has no usable residual data remaining and even advanced forensic tools should never be able to recover erased data.

Sanitization processes include any or all of the following: a software utility that completely erases the data; a separate hardware device that connects to the media being sanitized and erases the data; and/or a mechanism that physically destroys the device so its data cannot be recovered.

All University employees are responsible for notifying ITS or their appropriate ITC before:

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

2 Entities Affected by These Guidelines

The technical aspects of these guidelines apply to all ITS Baseline Services personnel and campus Information Technology Consultants who are responsible for ensuring that memory devices are sanitized according to these guidelines.

The responsibilities of these guidelines apply to Property Management who must ensure that data sanitization has occurred prior to disposition or donation of electronic storage media.

The responsibilities of these guidelines apply to all department administrators (MPP employees and department chairs) who must ensure that data sanitization has occurred prior to the relocation, reassignment, donation, or disposition of University-owned electronic storage media.

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, e-mail address, telephone number, date and place of birth, enrollment status, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, date of attendance, degrees and awards received, the most recent

educational agency or institution attended by the student, status as a student employee and department employed, if applicable.

b) Degaussing: The process of decreasing or eliminating an unwanted magnetic field on a hard drive, floppy disk or magnetic tape.

c) 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.

d) 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.

e) Level 1 Confidential Data: Confidential Information 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 information 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.

f) Level 2 Internal Use Data: Internal Use Information is information which 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 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.

g) Medical Information: Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

h) Memory Devices: Any drive, device, card, disk, computer tape, or other electronic medium that is used to store, copy, or preserve information, data, pictures, or graphics. Examples include: computer hard drives, magnetic disks, flash memory devices, CDs and DVDs, PDAs (e.g., Palm Pilots, Pocket PCs and Smart phones), Zip disks, digital camera memory cards; and USB storage devices (e.g., flash drives, iPods, and portable hard drives). Also called electronic storage media.

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:

   a. Social Security Number
   b. Driver's license or California Identification Card number

c. 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
d. Medical information
e. Health insurance information

j) 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.

k) Project Supervisor: Any ITS Baseline Services employee designated by the Assistant Director for Baseline Services to serve a lead role in a sanitization and refresh project assignment.

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.

4 Guidelines

University employees, in conjunction with their ITC, must ensure that all protected data in their possession is secure at all times. See the various User Guidelines cited in Section 7 - Related Documents for more information. Additionally, when memory devices are transferred between employees, departments or divisions, donated, or removed from service, all protected data must be sanitized prior to custody transfer. All such transfers require completion of the *Electronic Data Sanitization Verification* form.

ITS and ITCs are solely responsible for:

- Performing the data sanitization process on campus-owned computers and electronic storage media.
- Signing the *Electronic Data Sanitization Verification* form.
- Submitting the signed copy to Property Management (for donation or disposal) or the requesting department (for reassignment or relocation), as appropriate.

Memory device transfers between departments or divisions may or may not require ITS involvement. It is, therefore, imperative that ITCs and employees relinquishing custody of such devices take the necessary steps to sanitize all protected data on the device.

Removing an unsanitized hard drive prior to transferring, donating, or disposing of the computer or electronic storage device is not an acceptable practice. 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.

When computers and memory devices are disposed of or donated, copyright infringement of software licensing must be considered. All proprietary software applications or software applications that possess copy limitations must be removed prior to disposal or donation.

In the event of a memory device failure, all University employees must contact the ITS Help Desk for assistance. If replacement of the memory device is required without the need for recovery of data, ITS will attempt to remove any protected data before the memory device is returned. Memory devices containing protected data should never be returned directly to the vendor for replacement or taken to a computer store for repair or replacement. If, however, data recovery is required and the memory device must be sent to a third party vendor, the third party vendor must agree to and sign the University's *Information Confidentiality/Non-Disclosure Agreement* form found at http://www.calstatela.edu/its/forms. The agreement form must be attached to the *ITS Procurement Approval* form.

4.1 Data Sanitization Tools

Responsibility for data sanitization of all campus-owned memory devices is assigned to ITS and ITCs exclusively. However, all students, faculty, and staff are strongly encouraged to use these tools before exchanging, donating, or disposing of any **personal** memory devices.

4.1.1 Data Sanitization Utility for Windows, Unix/Linux, and PowerMac Systems

To assist the campus community in following data sanitization guidelines and best practices, employees can request a data destruction utility on a bootable CD (e.g., Darik's Boot & Nuke (DBAN) disk sanitization program) from the ITS Baseline Services Group. This application meets the requirements for performing data sanitization on Windows, Unix/Linux, and PowerMac-based platforms. Additionally, this open-source software application can be downloaded directly from http://dban.sourceforge.net.

4.1.2 Data Sanitization Utility on Apple-Macintosh Computer Systems

Apple Mac computer systems are shipped with an operating system reinstallation disk that contains an application named "Disk Utility". As an alternative to the procedure detailed in Section 4.1.1, this application can also be used to sanitize Mac systems. For best results, use the disks that were shipped with the system to ensure compatibility between the application and the operating system.

4.1.3 UNIX Based Computer Systems

The UNIX based operating system has the necessary software tools built-in to perform a sufficient sanitization process. Follow the step-by-step sanitization process available at the following location: http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/faqs/purge.xml.

4.1.4 Internal and External Hard Drive Destruction

There are several hardware tools available to destroy hard drives. A comprehensive list of currently recommended tools is available at http://www.calstatela.edu/its/desktop/datasanitization/.

4.1.5 Flash Drive Destruction

Either hardware or software tools can be used to securely sanitize flash drives. A comprehensive list of currently recommended tools is available at http://www.calstatela.edu/its/desktop/datasanitization/.

4.1.6 Physical Destruction

Physical destruction of media is the ultimate form of sanitization. Physical destruction can be accomplished using a variety of methods, including drilling holes in the device, or taking it apart and destroying individual components so that they cannot be reassembled. (Examples of tools that can be used for physical destruction include electric drills, pliers, etc.). All employees using tools to physically destroy media should follow all safety precautions, including wearing protective eye and hand gear.

4.2 Data Sanitization Procedures

Responsibility for data sanitization and refresh of campus-owned memory devices is assigned to ITS and ITCs exclusively. However, all students, faculty, and staff are strongly encouraged to follow these procedures before exchanging, donating, or disposing of any personal memory devices.

This section describes the detailed procedures involved in disk sanitization, depending on the type of platform or device.

- Sub-sections 4.2.1 through 4.2.3 explain the procedures for the three platforms: Windows, Unix/Linux, and PowerMac; Apple Macintosh; and UNIX.
- Sub-sections 4.2.4 through 4.2.6 outline procedures for the three main categories of Baseline refreshment where sanitization must be performed on a periodic basis: faculty and staff; electronic classroom and computer labs; and TEC rooms and lecture halls. The majority of such refreshments will be platforms running the Windows operating system.
- Sub-sections 4.2.7 through 4.2.12 outline procedures for miscellaneous memory devices.

4.2.1 Windows, Unix/Linux, and PowerMac Systems

Using the data destruction utility (e.g., Darik's Boot & Nuke (DBAN) disk sanitization program) described in Section 4.1.1:

1. Boot up the old computer or system using a bootable device other than the one to be sanitized.
2. Perform a low-level format with 7-pass wipe on the drive using Darik's Boot & Nuke utility software or the appropriate utility.
3. If protected data is present on the device, a 35-pass format must be performed with the Boot & Nuke utility. ITCs are responsible for assisting in identifying users with protected data on their system that may require a 35-pass format. This option is normally not performed if protected data isn't apparent due to the length of time required (up to one day).
4. On drives that cannot be sanitized due to the drive type (such as a SCSI drive or a defective device), the staff performing the sanitization will puncture two holes in the drive platters and the controller card.
5. Staff performing this sanitization procedure will complete the *Electronic Data Sanitization Verification* form available at: http://www.calstatela.edu/its/forms.
6. Department administrators are responsible for verifying the accuracy of the form and completion of the disk sanitization.

4.2.2 Apple-Macintosh Computer Systems

For Mac OS 10.4 or greater, using the Apple Mac operating system reinstallation disk described in Section 4.1.2:

1. Insert the Mac OS X "Install" disk that came with the computer, and then restart the computer while holding down the "C" key.
2. When the computer finishes starting up from the disk, choose "Disk Utility" from the "Installer" menu. (In Mac OS X 10.4 or later, select the language first.)
   Important: Do not click Continue in the first screen of the "Installer". If so, the process must be restarted from the disk again to access "Disk Utility."
3. Select the drive or volume to be sanitized.
4. Select "Erase."
5. Specify a volume format, and enter a name for the disk.
6. Click "Security Options" and select the "3-pass Erase" option for student machines, "7-pass Erase" option for faculty and staff machines, and "35-Pass Erase" option for specified machines with protected data.
7. Click "Erase."
8. Staff performing this procedure will complete the *Electronic Data Sanitization Verification* form available at: http://www.calstatela.edu/its/forms.
9. Department administrators are responsible for verifying the accuracy of the form and completion of the disk sanitization.

CAUTION

Equipment running Mac OS 10.3 or older only have the options to perform a 0-write wipe or an 8-pass wipe.

4.2.3 UNIX Based Computer Systems

Using the UNIX based operating system software tools described in Section 4.1.3:

1. As system administrator or security administrator, enter "format" either on the command line or in single-user mode.
2. When prompted, select the disk from the AVAILABLE DISK SELECTIONS. Enter the disk number.
3. Enter "defect" after the format> prompt.
4. Enter "primary" after the defect prompt to read in the manufacturer's defect list and update the in-memory defect list.
5. Enter "quit" to return to the main FORMAT MENU.
6. Enter "analyze."
7. Enter "purge," and when prompted, specify the slice that encompasses the entire disk.

CAUTION

This is slice 2 by default, but check this with the format command. At the top menu, choose the disk in question, then choose partition, and then choose print. One partition should start at the beginning of the disk and go all the way to the end. (Typically, but not always, this is named "backup".)

8. Enter "quit" to return to the main FORMAT MENU.
9. Enter "defect" after the prompt to return to the DEFECT MENU.

10. Enter “both” to update in-memory defect list with both the manufacturer's defect list and the grown defect list for another purge. This command also causes the combined defect list to be written to the working-list when you quit format.
11. Enter “quit” to return to the main FORMAT MENU.
12. Enter “analyze”.
13. Enter “purge”, and when prompted, specify a disk.
14. Enter “quit” to return to the main FORMAT MENU.
15. Enter “quit” to quit the format program.
16. Staff performing this procedure will complete the *Electronic Data Sanitization Verification* form available at: http://www.calstatela.edu/its/forms.
17. Department administrators are responsible for verifying the accuracy of the form and completion of the disk sanitization.

4.2.4 Faculty and Staff Refresh Preparation

1. Boot up the old computer or system using a bootable device other than the one being sanitized.
2. Perform a low-level format with 7-pass wipe on the drive using Darik’s Boot & Nuke utility software, or the appropriate utility (see Section 4.1.1, Data Sanitization Tools).
3. If protected data is present on the device, a 35-pass format will be performed upon request with the Boot & Nuke utility. ITCs are responsible for assisting in identifying users with protected data on their system that may require a 35-pass format. This option is not normally performed due to the length of time it takes, generally up to one day.
4. On drives that cannot be sanitized due to the drive type, such as a SCSI drive or a defective device, the staff performing the sanitization will puncture two holes in the drive platters and the controller card.
5. Staff performing this procedure will complete the *Electronic Data Sanitization Verification* form available at: http://www.calstatela.edu/its/forms.
6. The project supervisor is required to randomly verify the accuracy of the form and completion of the disk sanitization.

4.2.5 Electronic Classrooms and Computer Labs Refresh Preparation

1. Disk sanitization is scheduled 1-2 days before the computer refresh date.
2. The project supervisor will direct a team of Student Training Assistants (STAs) to perform proper disk sanitization procedures. All Electronic Classroom and Computer Lab computers will be sanitized using a 3-pass wipe with Boot & Nuke, or the appropriate utility (see Section 4.1.1, Data Sanitization Tools).
3. The project supervisor directs the STAs to complete the *Electronic Data Sanitization Verification* form available at: http://www.calstatela.edu/its/forms.
4. On drives that cannot be sanitized due to the drive type (e.g., SCSI drive or a defective device), the staff performing the sanitization will puncture two holes in the drive platters and the controller card.
6. The project supervisor is required to randomly verify the accuracy of the form and completion of the disk sanitization.

4.2.6 TEC Room and Lecture Halls Refresh Preparation

1. Computers that will be installed are prepared and delivered to the Media Services Group.

2. Media Services Group will return the old computer(s) to the Baseline Services Group upon completion of installation.
3. ITS Baseline Services staff will perform 3-pass wipe with the Boot & Nuke utility or the appropriate utility (see Section 4.1.1, Data Sanitization Tools).
4. On drives that cannot be sanitized due to the drive type (e.g., SCSI drive or a defective device), ITS staff will puncture two holes in the drive platters and the controller card.
5. Staff performing this procedure will complete the *Electronic Data Sanitization Verification* form available at: http://www.calstatela.edu/its/forms.
6. The project supervisor is required to randomly verify the accuracy of the form and completion of the disk sanitization.

4.2.7 External Hard Drives and Magnetic Disks

The following options are recommended:

1. Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) Web site at: http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml
2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved wand. Degaussing any current generation hard disk will render the drive permanently unusable.
3. Purge device by using agency-approved and validated purge technologies/tools. See Section 4.1.4 for recommended hardware tools.
4. Disintegrate, shred, pulverize or incinerate in a licensed incinerator.

NOTE

In the event that the Secure Erase software is unavailable, a comprehensive list of currently recommended tools can be found at http://www.calstatela.edu/its/desktop/datasanitization/.

4.2.8 Flash Drives and Flash Memory Sticks

Some flash drives have been known to retain their memory even after being submerged in water, cooked with propane, frozen in dry ice, submerged in various acidic liquids, run over with a Jeep, and fired against a wall with a mortar (Wikipedia). The only secure methods for removing data from flash drives are to utilize the hardware or software tools recommended at http://www.calstatela.edu/its/desktop/datasanitization/ or use the physical destruction methods outlined in Section 4.1.6.

To use the free Eraser software:

1. Download Eraser portable edition from http://portableapps.com/apps/utilities/eraser_portable.
2. Plug in the USB flash drive.
3. Delete all files and folders.
4. Run Eraser.
5. Create a new “On-Demand” task.
6. Run the task.
7. Format the USB flash drive.

NOTE

In the event that the Eraser software is unavailable, a comprehensive list of currently recommended tools can be found at http://www.calstatela.edu/its/desktop/datasanitization/.

4.2.9 CDs and DVDs

These devices should be shredded, disintegrated, pulverized, or incinerated.

4.2.10 PDAs

Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state. (The manufacturer should be contacted for proper sanitization procedures.)

4.2.11 Cell Phones

Manually delete all information, (e.g., calls made, phone numbers) and then perform a full manufacturer's reset to reset the cell phone back to its factory default setting. (The manufacturer should be contacted for proper sanitization procedures.)

4.2.12 Zip Disks

1. Degauss using a NSA/CSS-approved degausser. Degaussing any current generation zip disks will render the disk permanently unusable,
2. Incinerate disks and diskettes by burning the zip disks in a licensed incinerator, or
3. Shred.

5 Contacts

a) Address questions regarding this procedure to: ITInfrastructure@calstatela.edu.

b) Address questions regarding information security to: ITSecurity@calstatela.edu.

c) To request a copy of Darik's Boot & Nuke (DBAN) data destruction utility on a bootable CD, contact the ITS Baseline Services Group at ITInfrastructure@calstatela.edu.

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

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

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 This is a federal law that protects the privacy of student education records.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 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.
SB 1386	**California Personal Information Privacy Act, SB 1386** http://www.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.

7 Related Documents

The following documents, forms, and logs of the latest issue in effect shall apply to the extent specified herein.

ID/Control #	Title
ITS-1017-G	**User Guidelines for Safe Disposal of Electronic Storage Media** http://www.calstatela.edu/its/policies These guidelines outline the steps departments and business units, students, faculty, and staff should take to remove data and software and appropriately dispose of electronic equipment/devices.
ITS-1005-G	**User Guidelines for Portable Electronic Storage Media** http://www.calstatela.edu/its/policies 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-1008-G	**User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device** http://www.calstatela.edu/its/policies These guidelines outline the steps users must take to ensure the campus complies with all law and regulations regarding personal and confidential information when desktop or laptop computers and electronics storage devices are lost or stolen.
ITS-2006-G	**User Guidelines for Information Classification, Handling and Disposal** http://www.calstatela.edu/its/policies This guideline ensures that information on all media is classified, handled and disposed of in a secure manner.
ITS-2804	**Lost or Stolen Computer or Electronic Storage Device Report** http://www.calstatela.edu/its/forms This form must be completed immediately upon discovery of a lost or stolen device to ascertain whether protected data has been or is reasonably assumed to have been lost. State law requires notification to all persons impacted by such loss.
ITS-2808	**Information Confidentiality/Non-Disclosure Agreement** http://www.calstatela.edu/its/forms This form is designed for parties who need to work in areas that may contain protected data (Level 1 Confidential and Level 2 Internal User Information) and do not have an information confidentiality/non-disclosure agreement in place (e.g., contractual agreement, CSULA account).
ITS-8830	**Electronic Data Sanitization Verification** http://www.calstatela.edu/its/forms This form must be completed to authenticate the data sanitization process for every electronic storage device prior to relocation, reassignment, donation, or disposition.
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.