

<b>SANITIZING ELECTRONIC DATA STORAGE MEDIA PROCEDURE – UNIVERSITY OF TENNESSEE, KNOXVILLE AREA CAMPUS</b>	<b>REVISION NUMBER: DRAFT Revision 15</b>
<b>EFFECTIVE DATE: June 28, 2006</b>	<b>Page 1 of 4</b>

## OBJECTIVE

The [Sanitizing Electronic Data Storage Media Requirements](#) for the University of Tennessee, Knoxville Area campus covers the requirements for sanitization. It should be noted that proper sanitization of all information technology resources and the associated electronic data storage media is required in the following instances:

- Any system or associated electronic data storage media that is sent to the Surplus Property Division
- If the system or associated electronic data storage media is to be disposed of contains patentable, trade secret, or proprietary research records
- If the system or associated electronic data storage media was used in an area that handles Health Insurance Portability and Accountability Act (HIPAA) information
- If the system or associated electronic data storage media was used in an area that handles Gramm-Leach-Bliley Act (GLBA) information
- If the system or associated electronic data storage media was used in an area that handles Family Educational Rights and Privacy Act (FERPA) information
- If the system or associated electronic data storage media was used in an area that handles personally identifiable information as defined in state law Chapter Number 473, Senate Bill Number 2220

## 1. RESPONSIBILITIES

The [Sanitizing Electronic Data Storage Media Requirements](#) for the University of Tennessee, Knoxville Area campus covers the responsibilities of system/information owners and Surplus Sales personnel for sanitization.

## 2. RECOMMENDED METHODS OF SANITIZATION

All systems destined for surplus shall be sanitized by the Surplus Sales personnel **only** according to the [Procedure for Sanitizing Electronic Data Storage Media](#). Surplus Sales personnel are responsible for ensuring that all data and software are sanitized prior to a system's transfer off university property. Appropriate documentation shall be maintained for all systems processed through Surplus Sales.

### **Physical Sanitization (i.e. Physical Destruction)**

If the recommended software methods listed below are not able to remove the data, a computer will not boot, or the internal hard drive or drives are not accessible, then physical destruction is required. Drives and diskettes can be physically destroyed using a degausser. CDs, DVDs, and diskettes should be passed through a shredder. Physical destruction **IS NOT DEFINED** as throwing the medium in a trash can.

In cases where the system or associated electronic data storage media is being returned under warranty, the user must contact the vendor and establish the methodology for compliance with the sanitization requirements if there are none defined in the contract. Media with information covered under HIPAA, GLBA, FERPA, patentable, trade secret, proprietary research records, or state law Chapter Number 473, Senate Bill Number 2220 cannot be shipped to a vendor for exchange.

### **Software Assisted Sanitization of Computer Systems**

Assuming that the computer system will boot and all of the storage devices and media are accessible, the following procedures, depending upon the operating system, are recommended:

#### ***A. Solaris Based Computer Systems:***

The Solaris 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](http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/faqs/purge.xml)

#### ***B. Intel or AMD Based Computer Systems (includes Windows, Linux, and UNIX systems):***

The University of Tennessee has provided sanitization software tool for use by all university staff, faculty, and students called KillDisk. A copy of KillDisk can be obtained by qualified University technical staff by sending an email to [sanitize@utk.edu](mailto:sanitize@utk.edu). The Office of Information Technology (OIT) Business Office will burn a copy of the KillDisk software to a CD for use. If there are questions on sanitization of media, call the Information Security Office at 4-6555. If you have questions concerning the installation and usage of the KillDisk software, call the HelpDesk at 4-9900.

KillDisk runs in a command line environment and uses low-level access to the hard drives during the sanitization process. Therefore, an Intel or AMD based system can be sanitized using this tool, regardless of the installed operating system.

There are detailed instructions on the use of KillDisk provided in the User's Guide on the CD as well as posted on the <http://security.tennessee.edu> website. When you are asked for the "erase method", choose US DoD 5220.22-M.

#### ***C. Apple Mac Based Computer Systems:***

Apple Mac computer systems are shipped with an operating system reinstallation disk that contains an application named "Disk Utility". This application can 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.

The following instructions detail how to use the application, for Mac OS 10.4 or greater, once the system has been successfully booted to the reinstallation disk.

1. After the installer opens, select "**Utilities**" on the menu bar then select "**Disk Utility**" from the drop-down menu.
2. Select the drive to be sanitized. Be sure to select the entire drive.
3. Select "**Erase**" at the top of the window then select "**Security Options**" at the bottom of the window.
4. Select the "**35-Pass Erase**" option. Select "**OK**"
5. Select "**Erase**" at the bottom of the window then select "**Erase**" again.
6. When the erase is completed, select the drive again and select "**Erase Free Space**" to sanitize all deleted files.

#### ***D. Other Systems:***

Systems, media, or devices not covered under A, B, or C above must be sanitized utilizing the recommended tools provided by the manufacturer. This includes, but is not limited to, such systems as Advanced Interactive eXecutive (AIX), SGI, Storage Area Networks (SANS), Network Attached Storage (NAS), and tape drives.

**APPENDIX A**  
**UNIVERSITY OF TENNESSEE INFORMATION TECHNOLOGY SECURITY**  
**GLOSSARY OF TERMS**

**Electronic Information** – Refers to information in electronic form and the computer systems on which the information resides. This does not apply to information in paper form.

**Family Educational Rights and Privacy Act (FERPA)** – The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

**Gramm-Leach-Bliley Act (GLBA)** – Requires financial institutions, including universities, to protect the confidentiality and integrity of their customer's information.

**Health Insurance Portability and Accountability Act (HIPAA)** – Creates a standard for healthcare providers and institutions to protect the confidentiality and integrity of personal health information.

**Information Security Office** – The OIT entity that is responsible for the information technology security oversight and administration for the University of Tennessee.

**Information Technology Resources** – Includes any computers, computer systems, network devices, telephony systems, or software applications.

**Knoxville Area Campus** – The University of Tennessee, Knoxville Campus including all programs offered through UTK, the Institute for Public Service, the Institute of Agriculture, University Wide Administration physically located at the Knoxville campus, John XXIII, UT Battelle personnel located at the Knoxville campus, ERA modem pool users, DSL users, the Social Work Office of Research and Public Service (SWORPS) including Nashville locations.

**Personally Identifiable Information** – For this document is defined as an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements:

- Social security number;
- Driver license number; or
- Account number, 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.

**Sanitization** – is the process of erasing or destroying electronic data from IT equipment and associated storage media (hard drives, diskettes, tapes, CD-ROMs, DVDs, etc.) in a manner that gives reasonable assurance that the information cannot be recovered by any means.

**System/Information Owner** – Is the employee acting on the behalf of the University of Tennessee who bears responsibility for a particular set of University of Tennessee's information and associated computer systems that are under his or her control.

**Users** – Refers to all students, faculty, staff and others while accessing, using, or handling the University of Tennessee's information technology resources. "Others" includes, but is not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access.