

University of Utah Standard for Electronic Media Disposal

I. Overview

Data are being transmitted and stored on computer systems and electronic media by virtually every person conducting business for the University of Utah. Some of that data contains sensitive information, including student records, personnel records, financial data, and protected health information. If the information on those systems is not properly removed before the equipment is disposed of, or transferred within the University, that information could be accessed and viewed by unauthorized individuals. As such, all users of computer systems within the University of Utah, including contractors and vendors with access to University of Utah systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media are properly sanitized before disposal. Electronic Media is defined as any electronic storage device that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks and digital video disks. A wide variety of information resources contain electronic media including, but not limited to: computer systems, personal desktop assistants, smart phones, removable storage devices such as USB storage devices, copy machines and fax machines.

II. Purpose

The purpose of this standard is to establish procedures for the proper disposal of electronic media containing sensitive data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

III. Scope

The scope of this standard includes all individuals who are responsible for or who use University of Utah electronic media. Vendors and contractors who have access to University of Utah information resources are also subject to this standard. Disposal does not include media that contains data approved for release or sale by the University of Utah.

IV. Standard

A. Initiation

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

1) **Overwriting Media for Sanitization:** Overwriting is an approved method for sanitization storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. The University encourages use of certified sanitization software such as available through the Office of Software Licensing.

2) Destruction of Media: Destruction is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium, such as a computer, personal hand held device, audio or video player. The University encourages that destroyed media, such as hard drives, be processed through University Property Surplus or a "recycling agency" when appropriate.

All data governed by a data retention policy must be processed appropriately before the media on which it is stored is disposed of.

B. Disposal of Hard Drives

1) Transfer and disposal of hard drives to other departments or outside of the University of Utah: Prior to transfer, operable hard drives must be overwritten. Degaussing is not an effective means of data destruction on hard drives. Departments should maintain documentation of proper sanitization for hard drives; equipment designated for surplus or other disposal should have a label affixed stating that the hard drive has been properly sanitized.

2) Transfer of hard drives within a department: Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All hard drives should be sanitized, however; since the drive is remaining within the department, the hard drive may instead be formatted prior to transfer. Special recovery tools must be used by an individual to access the data erased by this method; any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the University of Utah Security Policy.

3) Sending a hard drive out for repair, return or for data recovery: The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with the University of Utah, insuring that the vendor will take proper care of the data. When possible, the vendor should return the defective media for proper disposal as described in this standard.

4) Disposal of damaged or inoperable hard drives: The owner must first attempt to overwrite the storage device. If the device can not be overwritten, the device must be disassembled and mechanically damaged so that it is not usable by a computer.

C. Disposal of electronic media other than hard drives

1) Transfer and disposal to other departments or outside of the University of Utah: All electronic media must be erased, degaussed, or rendered unusable before leaving the custody of its current user.

2) Transfer within a department: Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media should be erased if the media type allows it or destroyed if erasure is not possible.

D. Violation of Standard

If there is a reasonable basis to believe that the proper procedures as outlined in this standard have not been or are not being followed, a report must be filed with the Information Security Officer. If improperly sanitized electronic media is found, then the media should be reported to the appropriate departmental IT support personnel.