THE UNIVERSITY OF UTAH®

Title: Media Sanitization and Destruction
Number: G4-004N1
Responsible Office: Information Security and Privacy Office
Last Revision: April 2012
Owner: Director, ISPO. 801-587-9241 it_policy@utah.edu

I. OVERVIEW

A. The purpose of this document is to minimize the risks of exposing electronic data to individuals unauthorized to view that data and to avoid transferring software to those not licensed to use it. This policy is essential to compliance with state and federal data privacy statutes and with software licensing agreements.

B. It is also meant to provide guidance for the implementation of the University of Utah Information Security Policy – Section N(1)d: IT Resource Media Handling.

II. DEFINITIONS

A. Clear means to sanitize media by using software or hardware to overwrite storage space on the media with non-sensitive data at least 1 time. This includes overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also all addressable locations.

B. Purge means to sanitize media by using software or hardware to overwrite storage space on the media with non-sensitive data at least 3 times. This includes overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also all addressable locations.

C. Destroy means the result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover.

D. Electronic Media means all media on which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs, USB storage devices, and media within PCs, laptops, copiers, printers, etc.

III. GUIDELINES

A. Purge all software and data files from electronic media that are sent to University Surplus and Salvage, returned to a leasing company, or otherwise leaves the custody of the University. When electronic media is sent outside the University for repair, encrypt at University encryption standards or purge all data.

B. The approved procedures for software and data removal from electronic media are:

1. Except for these exceptions, destroy electronic media permanently leaving the University, or being disposed of:

a) Electronic media returned to a leasing company, from which all software and data files have been purged. Note: It is preferred that this media be destroyed.

b) Electronic media that have been encrypted to University encryption standards and whose encryption key has been destroyed.

c) See University Policy 3-041 at http://www.regulations.utah.edu/administration/3-041.html which requires that "equipment containing data storage devices must have those devices destroyed according to procedures established for that purpose."

2. When electronic media temporarily leaves the University for repair encrypt data at University encryption standards, purge, or remove the media.

a) If the purpose of the repair is to recover lost data from the media, please contact the Office of General Counsel or the Information Security and Privacy Office to ensure the appropriate contract is in place prior to sending or repairing the media.

3. Clear data from electronic media being transferred within the University (between departments or employees having different software and data access privileges).

a) Note: Securely store any electronic media awaiting processing under this guideline. Examples of secure storage include locking media in a closet, office or drawer.

C. Destroy paper containing restricted or sensitive information at end-of-life.

IV. REFERENCES

A. Health Insurance Portability and Accountability Act of 1996, "HIPAA" (PL 104-191)
B. HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164)
C. American Recovery and Reinvestment Act (PL 111-5), Title XIII – Health Information Technology, Section 13402
D. ISO 27001/2