UNIVERSITY of DENVER	**UNIVERSITY OF DENVER POLICY MANUAL DISPOSAL OF HARD DRIVE AND COMPUTER STORAGE MEDIA**

Responsible Department: Information Technology **Recommended By:** VC Information Technology and Chief Information Security Officer **Approved By:** Chancellor	**Policy Number** IT 13.10.030	**Effective Date** 10/__/2021

I. INTRODUCTION

University faculty and staff store sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media are phased out, sensitive information on the old equipment and media must be properly erased or otherwise made unreadable.

II. POLICY OVERVIEW

A. The University faces several risks related to the disposal of hard drives and other computer storage media:

- *Violation of Software License Agreements* - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Usually, these licenses are not transferable. Even when the licenses are transferable, there may be specific requirements that must be met, such as possession of the original distribution media, consent of the licensor, or payment of a transfer fee, in order to affect the transfer. Allowing a third-party access to licensed software without proper transfer of the license may be a breach of the license agreement and may subject the state or the recipient of the software to claims for damages.

- *Unauthorized Release of Confidential Information* - Allowing an unauthorized person access to confidential information can subject the University and sometimes individual employees, to claims for damages.

- *Unauthorized Disclosure of Trade Secrets, Copyrights, and Other Intellectual Property* – University computer systems develop and store data, programs, designs, techniques, etc., that are or will become valuable assets of the organization as either trade secrets, copyrighted materials, patented inventions, or other intellectual property. Accidental or premature disclosure could mean a loss of secrecy under trade secrets law or constitute a publication under federal copyright law, either of which might result in loss of the asset.

B. The Chief Information Security Officer shall ensure:

- Procedures address the final disposition of sensitive information, hardware, or electronic media.

- Procedures specify the process for making sensitive information unusable and inaccessible. Procedures specify the use of a technology (e.g., software, special hardware, etc.) to make sensitive information unusable, inaccessible, and not able to be reconstructed.

- Procedures specify the personnel authorized to dispose of sensitive information or equipment containing sensitive information. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed.

III. PROCESS OVERVIEW

A. The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled. Data can be present on any type of storage device, whether fixed or removable, that contains data and maintains the data after power is removed from the device. Due to the advances in computer forensics, simply deleting the data and formatting the disk will not prevent someone from restoring the data. However, sanitization of the storage media removes the information from the media in such a way that data recovery using common techniques or analysis is prevented.

B. Any and all computer desktops, laptops, hard drives, and portable media must be given to the IT Department for proper disposal. Paper and hard copy records should be disposed of in a secure manner as authorized by the Chief Information Security Officer

(CISO). The CISO's analysis of secure disposal processes should include, but not be limited to, shredders and storage of records in a secure area for an authorized disposal/recycling service.

C. Unless IT Department Staff can absolutely verify that no personal or confidential information, intellectual property, or licensed software is stored on the hard drive/storage media, the hard drive/storage media shall be sanitized or be removed and physically destroyed.

IV. DEFINITIONS

None

Revision Effective Date	**Purpose**