Removable Media Protection

I. Introduction

Managing the University data on removable media is an important part of the University's information security program. Today's removable media devices can store large quantities of data that could include sensitive data, and if inappropriately accessed or disclosed, could harm the reputation of the University. This policy outlines the expectations and requirements for the use and storage of University data on removable media.

II. Policy Overview

The University of Denver (University) must ensure adequate security of the information contained on removable media. All removable media containing University Data must be properly managed, protected, and securely disposed of to prevent unauthorized disclosure of sensitive information as required by IT 1.10.80 Information Security Policy.

This policy applies to all faculty and staff, contractors, consultants, temporary employees, partners, and third parties that use or have access to University Assets. This policy applies to IT systems owned or leased by the University or third-party systems residing at University facilities to support DU business operations.

Employees lacking clarity on how this policy affects their role at DU are encouraged to speak to their manager or a member of the Information Security (InfoSec) team.

III. Policy Process

A. Policy Statements

1. Information owner approval is required before University Data categorized as confidential or restricted can be stored on removable media. See IT 13.10.051 Data Classification Policy (not yet live, under review as of 11/7/22).
2. Only approved encrypted removable media devices must be used to store University Data.
3. All removable media shall be automatically scanned for malicious content when inserted into a University Asset.
4. When the information on removable media is no longer needed, it must be disposed of according to IT 13.10.030 Disposal of Information Policy.
5. When not in use, removable media shall be stored in a safe and secure environment.

6. Exceptions to this policy may be requested on a case-by-case basis by request to IT.

B. Roles and Responsibilities

1. The Information Security Office is responsible for this policy and its requirements.

IV. Definitions

- University Data
- University Asset
- Removable media - storage devices such as USB hard drives, thumb drives, CDs, backup media, and other media used to store and transport information in electronic format.