Procedure P4-004L: Media Handling

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this Media Handling Procedure is to outline the management, handling, and disposal processes for Media.

B. Scope.

The scope of this procedure is all University administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents.

This procedure supports Section L, titled Information System Media Handling, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this procedure. In addition, the terms below apply for the limited purpose of this procedure.

A. IT Resource Data Storage – Media on which an IT Resource's Information Assets are stored (e.g., hard drives and solid-state drives), which also includes Information System Media.

B. Least Privilege – The principle of granting Users the minimum access and authorization needed to perform their job functions.

C. Media – Information System Media, IT Resource Data Storage, and Removable Media.

D. Removable Media – Physical media that is attached to or easily removed from an electronic device (e.g., IT Resource, Information System, Workstation, Mobile Device) on which Information Assets are stored for backup and sharing purposes (e.g., USB drives, thumb drives, external hard drives, DVDs, CDs).

III. Procedure

A. Management of Media

1. IT managers shall:

   a. be knowledgeable of the applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations for the Media for which they are responsible;

   b. ensure Media is acquired from trusted sources;

   c. have a plan to ensure the confidentiality, integrity, and availability of Media;

d. at least annually, audit and review Media handling practices, plans, and procedures to identify and rectify any potential issues; and

e. consult the data owner before removing Information System Media from University premises.

2. IT Technicians shall:

a. implement all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations for the Media they manage;

b. store Media and documentation in accordance with all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations;

c. maintain an up-to-date inventory of all Information System Media containing Sensitive and Restricted Data;

d. label Information System Media and Removable Media with unique identifiers and data classification as required by any applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations;

e. maintain a detailed record of all Media containing Sensitive or Restricted Data removed from the University's premises;

i. Records shall include, at a minimum, the User who has possession of the Media, when it was removed from the University's premises, current Encryption state, and what data is stored therein.

f. implement strict access Control measures based on Least Privilege to ensure only authorized personnel have access to Information System Media;

g. encrypt all Media containing University data wherever technically feasible;

h. maintain Encryption keys in a secure location;

i. disable autorun, autoplay, and auto-execute functionality for Removable Media wherever technically feasible;

j. document usage of Information System Media; and

k. configure antivirus and anti-malware to scan Media at time of use.

B. Disposal of Media

1. IT managers shall:

a. retain Media disposal documentation in accordance with all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations.

2. IT Technicians shall:

a. safely and securely dispose of Media, at the direction of the data owner, when such Media is no longer required by any applicable federal, state, and local laws, regulations, and statutes, or contractual obligations; and

b. make unrecoverable the contents of Media containing Sensitive or Restricted Data prior to reuse or removal from the University's premises in accordance with all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations.

Sections IV- VII are for user information about this procedure.

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources

A. Policies/ Rules.

1. Policy 4-004: University Information Security Policy

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources.

1. NIST 800-88: Guidelines for Media Sanitization

V. References

[*reserved*]

VI. Contacts

The designated contact officials for this Regulation are

A. Policy Owner(s): primary contact person for questions and advice): Chief Information Security Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History.

A. Current version. Revision 0.

1. Approved by Chief Information Security Officer with effective date of November 6, 2024.

B. Renumbering

1. Not applicable