University Rule 4-004L: Information System Media Handling Rev. 0

I. Purpose and Scope

A. The purpose of this Information System Media Handling Rule is to protect the University's physical Information System Media from unauthorized disclosure, modification, removal or destruction.

B. This Rule supports section L, titled Information System Media Handling, of the University of Utah Information Security Policy 4-004.

II. Definitions

For the purposes of this Policy and any associated Regulations, these words and phrases have the following meanings:

A. **Confidential** - Any Information Asset which is classified as Restricted or Sensitive per the Data Classification and Encryption Rule

B. **Information System Media** -Physical media on which an Information System's Information Assets are stored for backup and recovery purposes (e.g. backup tapes, backup disks, NAS/SAN drives, magnetic media, etc.).

C. **IT Technicians** – IT Technicians develop, administer, manage and monitor the IT Resources, Information Systems, and Electronic Resources that support the University's IT infrastructure, are responsible for the security of the IT Resources, Information Systems, and Electronic Resources they manage, and assure that security-related activities are well documented and completed in a consistent and auditable manner.

III. Rule

A. Management of Information System Media

When managing the University's Information System Media, IT Technicians will:

1. Store Information System Media in a safe, secure environment

2. Require authorization prior to removing Information System Media from the University's premises, and maintain a detailed record of all authorized removals

3. Delete, or otherwise make unrecoverable, the contents of re-usable Information System Media containing Confidential data prior to removal from the University's premises if the contents are no longer required in accordance with the Data Classification and Encryption Rule

4. Wherever technically feasible, encrypt all Information System Media containing data in accordance with Data Classification and Encryption Rule

B. Handling of Information System Media Data

1. The University will document and follow approved procedures and methodologies for handling Information System Media in accordance with the classification of the data stored on the Information System Media

C. Disposal of Information System Media

1. The University will dispose of Information System Media safely and securely when such media is no longer required, following approved procedures and methodologies

2. Disposal of Confidential data should be conducted in accordance with the Data Classification and Encryption Rule, and logged where possible in order to maintain an audit trail

[Note: Parts IV-VII of this Rule (and all other University Regulations) are Regulations Resource Information--the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined

appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

I. Rules, Procedures, Guidelines, Forms and other Related Resources

A. Rules

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

TBD

D. Forms

E. Other Related Resources Material

II. References

A. 45 C.F.R. 164: Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy

B. Family Educational Rights and Privacy Act of 1974 ("FERPA", 20 U.S.C. § 1232g)

C. Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541)

D. ISO 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls

E. NIST 800 Series, Federal Information Security Standards

F. Policy 3-070: Payment Card Acceptance

G. Policy 4-001: University Institutional Data Management

H. Policy 4-003: World Wide Web Resources Policy

I. Policy 5-111: Disciplinary Actions and Dismissal of Staff Employees

J. Policy 6-400: Code of Student Rights and Responsibilities

K. Policy 6-316: Code of Faculty Rights and Responsibilities

L. Pub. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

M. Omnibus HIPAA Rule: 45 CFR Parts 160 and 164 - Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

III. Contacts

A. The designated contact Officials for this Policy are:

1. Policy Owner (primary contact person for questions and advice): Chief Information Security Officer, 801-213-3397

2. Policy Officer; Chief Information Officer, 801-581-3100

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases...."

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library.... [and] bears the responsibility for determining -requirements of particular Policies...." University Rule 1-001-III-B & E

IV. History

A. Current version: Revision 1, effective date: April 4, 2016

Approved by Academic Senate: May 4, 2015

Approved by Board of Trustees: May 12, 2015

Background information for this version