University Rule 4-004O: Security Awareness and Training Rev. 0

I. Purpose and Scope

A. The purpose of this Security Awareness and Training Rule is to outline the approach that the University will follow to provide Security education to Users of the University Information Systems. The education will consist of both Security Awareness education and Security Training.

B. This Rule supports section O, titled Security Awareness and Training, 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. **Information Asset** - Data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling University to perform its business functions.

B. **Information System** - An Application or group of Servers used for the electronic storage, processing, or transmitting of any University data or Information Asset.

C. **Restricted Data** – Any data types classified as Restricted per the Data Classification and Encryption Rule.

D. **User** – Any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third party agents, who accesses any University Electronic Resources, Information Systems, and/or IT Resources.

III. Rule

A. Security Awareness

1. All Users will be provided with security awareness training. Awareness training will be provided through a number of different forums:

    a. New employee orientation

    b. Annual regulatory compliance training

    c. Security articles in various newsletters

    d. Periodic security reminders

    e. Email or other mass notification of substantial changes to University regulations.

2. The purpose of the University's Security Awareness program is to educate its workforce to recognize key security concerns and to respond accordingly. Key security concerns include:

    a. Protecting the University Information Systems and Information Assets against malicious software and exploitation of vulnerabilities

    b. Identifying and reporting security incidents

    c. Understanding applicable regulatory compliance requirements

    d. Understanding on-going changes in technologies and security practices

3. Information security program documentation will be available to all Users and will be stored in a location that can be easily accessed.

B. Security Training

1. The University's security training program and training materials will incorporate relevant security topics, will be reviewed periodically to ensure the

training is current, and will be approved by the Chief Information Security Officer prior to being presented.

2. Security training attendance and completion will be recorded.

3. All Users must complete appropriate security training without unreasonable delay prior to accessing any University Information System containing Restricted data.

4. The University will identify personnel that have significant Information System security roles and responsibilities, document those roles and responsibilities, and provide security training as necessary to these personnel in order to fulfill security responsibilities.

5. Some positions may have specific security training and/or certification requirements.

    a. Any certification requirements or training requirements will be defined in the job description.

        i. For employees with specific security responsibilities, security skill competency may be measured during the annual performance evaluation.

    b. An action plan will be developed as necessary and may involve additional security training.

    c. Specific security training may be provided through a number of different forums, including but not limited to:

        i. User group meetings.

        ii. Formal security education.

        iii. Security publications.

[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