# University Rule 4-004N: Information Security Incident Management Rev. 0

## I. Purpose and Scope

A. The purpose of this Information Security Incident Management Rule is to ensure that information security incidents are communicated in a timely manner to the appropriate personnel, and to ensure that the personnel responsible for responding to and mitigating information security incidents follow consistent and effective processes and procedures.

B. This Rule supports section N, titled Information Security Incident Management, 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 Security Incidents** - Events or weaknesses that jeopardize the confidentiality, integrity, and availability of the University's Information Assets, IT Resources, and Information Systems.

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

D. **IT Resource** – A Server, Workstation, Mobile Device, medical device, networking device, web camera or other monitoring device, or other device/resource that is a) owned by the University or used to conduct University business regardless of ownership; b) connected to the University's network; and/or c) that is creating,

accessing, maintaining, or transmitting Information Assets and used for electronic storage, processing or transmitting of any data or information.

E. **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. Information Security Incident Identification and Reporting

All University Users must report any observed or suspected Information Security Incidents upon discovery and as quickly as possible to their respective helpdesk via phone call, email, or other automated method. The University will develop and communicate Information Security Incident response reporting procedures that include the following key elements:

1. Examples of information security events or incidents
2. Information Security Incident reporting forms, in an easily accessible format, to assist the reporter with capturing all of the pertinent details of the incident
3. Feedback processes to notify Information Security Incident reporters of the status of the incident investigation and the investigation results as appropriate.

B. Information Security Incident Management

The University will establish and communicate procedures for managing Information Security Incidents effectively once they have been reported, and these procedures must include the following key elements:

1. Clearly defined roles and responsibilities for both management and response personnel

2. Methods for detecting Information Security Incidents
3. Procedures for the collection, retention and presentation of evidence
4. Mechanisms for monitoring and quantifying the impact of Information Security Incidents
5. Document lessons learned to report on the effectiveness of current incident management procedures, and identify necessary improvements to existing security controls and practices.

*[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