Rule 4-004B Information Security Risk Management, Rev. 2

I. Purpose and Scope

A. The purpose of this Information Security Risk Management Rule is to establish the University's risk management program. The objective of University's Risk Management Program is to support University's core institutional and research missions as well as patient safety and quality of care goals, while also mitigating financial, operational, reputational and regulatory compliance risk. This Information Security Risk Management Rule shall enable the University to accomplish its missions by:

1. Securing the Information Systems that create, maintain, process, or transmit University data designated as "Restricted" or "Sensitive" per the University's Data Classification and Encryption Rule.

2. Enabling the appropriate University personnel to make well-informed decisions regarding risk and risk management.

B. This Rule supports section B, titled Information Security Risk Management, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004: University of Utah Information Security Policy, apply for purposes of this Rule, including the following:

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

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. **Risk** - Risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. Risk is usually calculated as either a quantitative or qualitative score, and can be represented in the following equation: Risk = (Likelihood of Threat/Vulnerability Event Occurrence) X (Business Impact of Event Occurring)

Inherent Risk – Inherent Risk is defined as the likelihood and impact of loss arising out of circumstances or existing in an environment, IT Resource, or Information System in the absence of any action to control or modify the circumstances.

Residual Risk – Residual Risk is the risk of an IT Resource that remains after controls or other mitigating factors have been implemented.

E. **Sensitive Data** – Any data type classified as Sensitive per the Data Classification and Encryption Rule.

F. **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. The University's information security risk management methodology is based foremost on the National Institute of Standards and Technology (NIST) Special Publication 800-30 "Risk Management Guide for Information Technology Systems" methodology.

B. The University leverages numerous government and industry recognized information security control frameworks depending on the situation, risk tolerance, data types, and as specified in applicable regulations.

1. For questions regarding information security control frameworks and what is applicable to the situation in question, please contact the Information Security office at iso-grc@utah.edu or ciso@utah.edu.

C. Risk Assessment

1. Inherent risk scores are calculated based on the following five (5) vectors of risk, which assess both the likelihood and impact of compromise:
    a. Impact: The number of Users who access the Information System
    b. Impact: The number of individual data records stored on the Information System
    c. Likelihood: The type of architecture that Information System employs
    d. Likelihood: The types of Users that access the Information System
    e. Likelihood and Impact: The highest classification of data the Information System creates, maintains, processes, or transmits
2. Residual risk scores are calculated based on the inherent risk score and the percentage of compliance of the control objectives assessed during a full risk assessment. A full risk assessment includes the following elements:
    a. Entity level controls
    b. System level controls

D. Risk Management

The appropriate University key stakeholders shall be issued both Inherent and Residual Risk scores in risk assessment summary reports for all Information Systems assessed. These stakeholders will be responsible for either formally accepting the risk of operating the Information System in the University's environment, or rejecting the risk and requiring a formal corrective action plan to

allocate the appropriate timelines, budget line items, and/or other resources to remediate control failures and reduce the Residual Risk score to an acceptable level for the University.

[Note: Parts IV-VII of this Regulation (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.]

IV. 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

V. 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

N. Cyber Security Framework: The Cyber Security Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk

VI. 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

VII. 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