University Rule 4-004I: Network Security Rule Rev. 0

I. Purpose and Scope

A. The purpose of this Network Security Rule is to protect the University's Information Assets and Information Systems within its network, and to protect the supporting network infrastructure.

B. This Rule supports section I, titled Network Security, 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. **Electronic Resource** - Any resource used for electronic communication, including but not limited to internet, Email, and social media.

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. **Server** - Hardware and software and/or Workstation used to provide information and/or services to multiple Users.

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. Network Controls

To protect the University from threats and to maintain security for IT Resources, Information Systems, Electronic Resources, Users and applications utilizing the University network, the University's network will be adequately managed and controlled, taking into consideration the following:

1. The operational responsibility for managing the University's network will be separated from computer operations where possible.

2. Additional confidentiality and integrity controls will be implemented commensurate with risk to protect Confidential data passing over public networks or wireless networks, and to protect the connected Information Systems.

3. Risk assessment and risk management activities will incorporate the business requirements of network availability as well as the security requirements to protect the University's network from threats. Risk remediation activities must be monitored periodically to ensure that control implementation is consistent across the University's network infrastructure.

B. Network Service Agreements

1. The University will identify and include required security features, service level expectations, and network security management requirements in all network services agreements.

2. Network services include network connection provisioning, private network services, and managed network security solutions such as firewalls and intrusion detection and prevention systems.

3. Both in-house and outsourced services must be captured in these agreements

C. Network Segregation

The University will segregate groups of Information Assets, IT Resources, Servers, Information Systems, and Users within its network. The University will consider the following strategies when implementing network segregation, defined by a risk assessment, and protected by a defined security perimeter:

1. Logical network domains, such as:

   a. Internal network domains

   b. External network domains

   c. Publicly accessible systems

   d. Wireless networks

2. Network device functionality, such as:

   a. IP switching

   b. Routing

   c. Information Assets stored or processed on the network

   d. Data classification

   e. Data value

   f. Business impact

3. The network security perimeters will be implemented via an installed security gateway between interconnected networks, configured to:

    a. Control access and information flow between the domains

    b. Filter traffic between the domains

    c. Block unauthorized access

4. Network Connection Controls

    a. Where technically feasible, the University will restrict the capability of Users to connect to the network in accordance with the minimum business requirements of each User's job function by utilizing role-based access.

    b. These network connections will be restricted by security gateways that filter traffic in accordance with pre-defined tables or rules.

5. Network Routing Controls

    a. The University will implement routing controls for its network as defined by risk assessments.

[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.]

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 Material

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

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