University Rule 4-004H: Remote Access Rev. 0

I. Purpose and Scope

A. The purpose of this Remote Access Rule is to protect the University's IT Resources, Information Systems, and Information Assets when accessed remotely. This Rule applies to remote access connections used to perform work for or on behalf of the University.

B. This Rule supports section H, titled Remote Access, 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. **Dual-homing** - A term used to reference a fault-tolerant scheme that uses more than one network interface.

B. **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.

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. **Remote Access** - Enables Users to send and receive data across shared or public networks as if their IT Resources were directly or virtually connected to the University's trusted network, and thus are benefiting from the functionality, security and management policies of the University's trusted network.

F. **Split-tunneling** - A computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local area network or wide area network at the same time, using the same or different network connections.

G. **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.

H. **VPN** - A Virtual Private Network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the University's network.

III. Rule

A. Remote User Access Methods

1. All remote access methods are covered by this Rule. Remote access methods include but are not limited to, Citrix, Remote Desktop Protocol (RDP), Secure Shell (SSH), and VPN.

B. Remote Access User Responsibilities

Users with remote access privileges are responsible for the following:

1. Ensuring that the remote access connection is given the same consideration as the User's on-site environment.

2. Complying with all University regulations.

3. Ensuring their remote access session is restricted to only their use and that it is not used by others.

C. Remote Access Requirements

Prior to issuing access to the University's remote access technologies, the following requirements must be met:

1. Remote access must be strictly controlled, and at minimum require the use of unique User credentials and authentication.

2. Remote access authentication methods are to be used only by the User to whom they were assigned and shall not be shared.

3. All remote access connections must utilize a University-approved form of encryption in accordance with the Data Classification and Encryption Rule's requirements.

4. Overriding or altering the configuration of the remote access connection that results in a compromise of the security of the University's trusted networks is prohibited. For example, reconfiguration of a remote User's IT Resource for the purpose of Split-tunneling or Dual-homing is not permitted at any time.

5. All IT Resources that are connected to the University's internal network via remote access technologies must have up-to-date anti-malware software implemented.

[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 Resource Materials

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