University Rule 4-004G: IT Resource and Information System Security and Vulnerability Management. Rev. 0. Effective Date: April 4, 2016

I. Purpose and Scope

A. The purpose of this IT Resource and Information System Security and Vulnerability Management Rule is to protect the University's IT Resources and Information Systems, detect and remediate security vulnerabilities, and ensure that IT Resources and Information Systems are available for authorized use.

B. This Rule supports section G, titled IT Resource and Information System Security and Vulnerability 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 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 Technicians** - IT Technicians develop, administer, manage and monitor the IT Resources, Information Systems, and Electronic Resources that support the University's IT Infrastructure, are responsible for the security of IT Resources, Information Systems, and Electronic Resources they manage, and assure that security-related activities are well documented and completed in a consistent and auditable manner.

E. **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.

F. **Mobile Code** - Software transferred between IT Resources and executed on a local system without explicit installation or execution by the recipient. Examples include, but are not limited to, scripts such as JavaScript or VBScript, Java applets, ActiveX controls, Flash, and macros embedded in Microsoft Office documents.

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.

III. Rule

A. IT Resource Classifications

1. The University will classify IT Resources by type based on the ownership, function, and physical location.

2. The University will analyze the physical surroundings of IT Resources to prevent and preclude unauthorized access, and limit the ability of unauthorized persons to view Confidential information.

B. Anti-Virus and Endpoint Security

To protect the confidentiality, integrity and availability of IT Resources, Information Systems, and Information Assets, the University implements anti-malware detection, prevention, and recovery controls. The following controls will be implemented:

1. The use and/or installation of unauthorized software shall be strictly prohibited.

2. Periodic Information Asset and software inventory reviews will be conducted to detect the presence of unapproved files and unauthorized software installations.

3. Anti-malware and/or endpoint security tools shall be installed and configured to automatically update regularly on all IT Resources and Information Systems.

4. Anti-malware and/or endpoint security scanning must be configured to run automatically.

5. IT Technicians should subscribe to reputable sources to receive notifications for warning bulletins, and notifications to differentiate between hoaxes and verifiable malicious codes.

C. Vulnerability Management

1. To assess and apply appropriate security patches that impact IT Resources and Information Systems, the University will monitor vendor and third-party sources for updated vulnerability information and distribute pertinent patch information to responsible parties without unreasonable delay.

2. The University will utilize automated assessment tools to identify vulnerabilities or configuration issues on all IT Resources and Information Systems connected to the University's network.

3. The University will classify vulnerabilities according to the following severity levels, and align these classifications with proprietary vulnerability management tool scores as appropriate:

   a. Urgent – The "Urgent" classification applies to broad threats to the University or remotely exploitable vulnerabilities through which an intruder can easily gain control of numerous Information Systems, gain full read and write access to files, remotely execute commands, exploit backdoors, or cause wide-spread service interruption. Intruders can easily gain control of the host, which can lead to the compromise of the University's entire network security. Vulnerabilities assigned a rating of "Urgent" must be remediated within 72 hours of discovery.

   b. Critical – The "Critical" classification applies to vulnerabilities through which an intruder can possibly gain control of one or more Information Systems, gain full read access to files, potential backdoors, a listing of all the users on the host, or there may be potential leakage of Confidential information. This includes local exploits where the risk of compromise is not as high as an Urgent vulnerability. Vulnerabilities assigned a rating of "Critical" must be remediated within 15 days of discovery.

   c. Serious – The "Serious" classification applies to vulnerabilities that may allow an intruder to gain access to a partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. Vulnerabilities assigned a rating of "Serious" must be remediated within 30 days of discovery.

   d. Medium – The "Medium" classification applies to vulnerabilities that may allow an intruder to gain access to Information Assets stored on an

Information System, or collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Vulnerabilities assigned a rating of "Medium" must be remediated within 60 days of discovery.

e. Low – The "Low" classification applies to vulnerabilities that do not pose an immediate threat to the University Information Systems. Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. Vulnerabilities assigned a rating of "Low" should be remediated within 90 days of discovery.

4. In a situation where a patch cannot be installed due to incompatibility with an IT Resource or Information System, testing requirements, or other pertinent patching limitations, an exception must be filed within the same required timeframe for remediation.

D. Patch Management

1. When a vendor releases a patch or update to repair a security-related control, the release shall be considered an implicit vulnerability notification and risk mitigation shall be taken.

2. All patch and update procedures shall be conducted in accordance with the University's Change Management Rule and Procedures.

3. IT Technicians should install patches on a non-production system, if available, to verify that the security patch will not adversely impact system functionality.

4. Software assets shall be inventoried to ensure that known vulnerabilities can be readily identified by IT Technicians tasked with vulnerability management.

5. IT Resources and Information Systems shall be hardened in accordance with applicable industry best security practices prior to release into the production environments.

6. Mitigation procedures shall be put into place in the event that vulnerabilities are exploitable and/or exploited before they can be removed from the environment.

7. When appropriate, security monitoring and scanning tools shall be used to verify that remediation activities have been performed and a new vulnerability baseline shall be created.

8. Configuration procedures, hardening scripts, inventories, etc. shall be updated as required to reflect the current IT Resource or Information System state (after the vulnerability has been remediated). Procedures shall prevent new IT Resources and Information Systems from being deployed with existing vulnerabilities.

E. Operating System Access Controls

To prevent unauthorized access to IT Resources and Information System operating systems, the University will implement the following controls for ensuring a secured log-on procedure:

1. Provide appropriate means for authenticating authorized Users

2. Limit the number of unsuccessful log-on attempts

3. Record unsuccessful log-on attempts

4. Auto-lock and/or auto-logoff sessions due to inactivity

5. Issue alarms when security requirements are breached

F. Mobile Code Controls

1. To protect against mobile code performing unauthorized actions, the following controls should be considered:

   a. Manage the use of mobile code where it is prohibited

   b. Manage the receipt of mobile code where it is prohibited

   c. Control the resources available to mobile code access

   d. Employ encryption controls to uniquely authenticate mobile code

[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

[reserved]

B. Procedures

Procedure: Support for 4-004G: IT Resource and Information System Security and Vulnerability Management

C. Guidelines

[reserved]

D. Forms

[reserved]

E. Other related resource materials

[reserved]

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