Rule R4-004G: IT Resource and Information System Security and Vulnerability Management

Revision 1. Effective date: September 12, 2023

I. Purpose and Scope

A. Purpose

The purpose of this rule is to outline the University's process, owned by the Information Security Office, for the identification, assessing, notification,

managing, and remediating of cybersecurity Vulnerabilities across Information Systems and IT Resources.

B. Scope

The scope of this rule is all University administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents.

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 apply for this rule. In addition, the terms below apply for the limited purposes of this rule:

A. 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 (e.g., JavaScript, VBScript), Java applets, and macros embedded in Microsoft Office documents.

III. Rule

A. Workstation and Server Security

1. Users and/ IT Technicians shall install and use security tools as required by the Information Security Office and may not install other software that conflicts with, impedes, obstructs, or disables those tools.

B. Vulnerability Management

1. To assess and apply appropriate security Patches that impact IT Resources and Information Systems, IT Technicians shall monitor vendor and third-party sources for updated Vulnerability information and implement Patches and/or mitigating Controls in accordance with the Vulnerability classification listed in

this rule. See supporting Procedures in this Rule for more information about Vulnerability Management.

2. IT Technicians shall use automated assessment tools to identify Vulnerabilities or configuration issues on all IT Resources and Information Systems connected to the University's network.

3. IT Technicians shall subscribe to reputable sources to receive notifications for Patches, security updates, and warning bulletins about hoaxes, scams, fraud, and malicious software.

4. The University uses the National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) for Vulnerability classification. The following are the CVSS severity rankings and the University's mitigation time frames:

    a. Critical: Must be remediated within 72 hours of discovery.

    b. High: Must be remediated within 15 days of discovery.

    c. Medium: Must be remediated within 30 days of discovery.

    d. Low: Must be remediated within 60 days of discovery.

    e. None: Must be remediated within 90 days of discovery.

5. 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 to policy shall be filed by the User or IT Technician as described in Policy 4-004 within the same required time frame for remediation.

C. Patch Management

1. IT Technicians shall consider a Patch or update to repair a security-related Control released by a vendor to be a Vulnerability notification and shall undertake appropriate risk mitigation.

2. All Patch and update procedures shall be conducted in accordance with the Procedure P4-004E.
3. IT Technicians shall install Patches on a non-production or test system to verify that the security patch will not adversely impact system functionality.
4. IT Technicians shall inventory software assets to ensure that known Vulnerabilities can be readily identified and remediated.
5. IT Technicians shall use Security Baselines to configure IT Resources and Information Systems in accordance with University procedures prior to release into the production environments.
6. IT Technicians shall mitigate Risk from Vulnerabilities that are exploitable and/or exploited before they can be removed from the environment.
7. IT Technicians shall verify that remediation activities have been performed and are functioning as expected.
8. IT Technicians shall have all operating system and Application patches installed before deploying new IT Resources and Information Systems.
9. New IT Resources and Information Systems may not be deployed with end-of-life or end-of-support operating systems or Applications.

D. Operating System Access Controls

To provide a secure log-on procedure and prevent Unauthorized Access to IT Resources and Information Systems, IT Technicians shall implement the following Controls:

1. limit the number of unsuccessful log-on attempts;
2. record unsuccessful log-on attempts;
3. auto-lock and/or auto-logoff sessions due to inactivity; and
4. issue alarms when security requirements are breached.

E. Mobile Code Controls

To protect against Mobile Code performing unauthorized actions, IT Technicians shall implement the following Controls:

1. manage the use of Mobile Code where it is prohibited;
2. manage the receipt of Mobile Code where it is prohibited;
3. control the resources available to Mobile Code access; and
4. employ encryption controls to uniquely authenticate Mobile Code.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

IV. Policies/ Rules, Procedures, Guidelines, Forms, and other Related Resources

A. Policies/ Rules.

1. Policy 4-004: University of Utah Information Security Policy

B. Procedures, Guidelines, and Forms.

C. Other Related Resources. [*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: 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. Utah Board of Higher Education Policy R345: Information Technology Resource Security

VI. Contacts

The designated contact officials for this Regulation are:

A. Policy Owner(s) (primary contact person for questions and advice): Chief Information Security Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History

A. Current version. Revision 1.

1. Approved by President Randall as an Interim Rule on September 12, 2023 with effective date of September 12, 2023. Rule finalized with no changes after Board of Trustees approval of Policy 4-004 revisions on November 14, 2023.
2. Legislative History
3. Editorial Revisions

B. Previous versions.

1. Revision 0. Effective date April 4, 2016.

C. Renumbering

1. Not applicable.