Rule R4-004J: Log Management and Monitoring

Revision 1. Effective date: September 12, 2023

I. Purpose and Scope

A. Purpose.

The purpose of this Log Management and Monitoring Rule is to protect the University's Information Systems by establishing requirements for the configuration and review of Information System activities through Log management and monitoring.

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 J, titled Log Management and Monitoring, 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 purpose of this rule.

A. Least Privilege – The principle of granting Users the minimum access and authorization needed to perform their job functions.

III. Rule

A. Logging

1. To detect unauthorized activity and assist in future investigations for Information Systems, Logs must capture the following information:
    a. User ID;
    b. User login and logoff date and time with IP address;
    c. successful and unsuccessful login attempts;
    d. file system, application, and operating system configuration changes;
    e. system utility use;
    f. activation and deactivation of security mechanisms such as logging, anti-malware, and/or management agents; and
    g. actions taken by Users logged in as an administrator.

2. When required, IT Technicians shall implement additional logging Controls as identified by contractual obligation or applicable regulatory body.

B. Review of Logs

1. IT Technicians shall periodically review on a continuous basis, either manually or by automation and in accordance with published procedures, Logs for Information Systems that create, store, process, or transmit University Information Assets.

C. Protection of Log Information

1. Logs must be protected from tampering. Access must be based on the principle of Least Privilege. IT Technicians are accountable for the integrity of Logs for the Information Systems they are responsible for.
2. Read/write access to the Log files shall be limited to authorized personnel.
3. IT Technicians shall monitor read/write access of the Log files by authorized personnel.

D. Hardware Fault Logging

1. IT Technicians shall take appropriate action on Information System and Server hardware faults and implement the following Controls:
   a. enable fault logging;
   b. enable automatic alerts for critical system fault Logs; and
   c. regularly review fault Logs and correlation with fault resolutions.

E. Clock Synchronization

1. IT Technicians shall ensure Information Systems are synchronized to the authoritative University time source.

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. [*reserved*]

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 6, 2016

C. Renumbering

1. Not applicable