University Rule 4-004J: Log Management and Monitoring Rev. 0

I. Purpose and Scope

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

B. This Rule supports section J, titled Log Management and Monitoring, 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. **Application** - Any individual or standalone piece of software that is used to provide a specific service to a community of users, or is used as an interface to an Information System.

B. **Confidential** - Any Information Asset which is classified as Restricted or Sensitive per the Data Classification and Encryption Rule

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

III. Rule

A. Audit Logging

In order to detect unauthorized activity and assist in future investigations for Information Systems that create, store, process or maintain Confidential data, the following controls must be implemented for Information System audit logs:

1. Audit logs should record user activities, password events, and information security events, commensurate with the assessed level of risk.
2. Audit logs must capture the following information:
    a. User ID
    b. User login and logoff dates and times
    c. Successful and unsuccessful login attempts
    d. Successful and unsuccessful file permission changes and/or access attempts and type of access, to include:
        i. Read
        ii. Write
        iii. Modify or Update
        iv. Delete
    e. System configuration changes
    f. System utility use

g. Activation and de-activation of security mechanisms such as audit logging, anti-malware, and/or management agents

B. Review of Audit Logs

1. Audit logs for Information Systems that create, store, process or maintain Confidential data shall be reviewed periodically in accordance with published Procedures, and at a minimum on a quarterly basis.

C. Protection of Log Information

In order to maintain the confidentiality and integrity of audit logs for Information Systems that create, store, process or maintain Confidential data from unauthorized access and tampering, the following controls must be implemented:

1. Control read/write access to the log files to a limited group of authorized personnel

2. Monitor read/write access of the log files by authorized personnel

D. Administrator and Operator Logs

In order to monitor the activity of IT Technicians and other system administrators on Information Systems that create, store, process or maintain Confidential data, the following controls must be implemented:

1. Administrator logs must include the following:

a. Date and time of administration event

b. Administrator login id used

c. Event transaction details

d. Service and/or process activation or de-activation

2. Administrator logs will be reviewed periodically in accordance with published Procedures.

E. Hardware Fault Logging

In order to take appropriate action on Information System and Server hardware faults, the following controls must be implemented:

1. Fault logging must be enabled
2. Enable automatic alerting for critical System fault logs
3. Fault logs will be reviewed regularly and correlated with fault resolutions

F. Clock Synchronization

In order to ensure the accuracy of audit logs, the following controls must be implemented:

1. The clocks of all University Information Systems and Servers capable of creating logs must be synchronized to an authoritative Coordinated Universal Time source.

[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