Procedure P4-004J: Log Management and Monitoring

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this Log Management and Monitoring Procedure is to outline a structured, efficient approach for generating, transmitting, storing, and analyzing Log data as a means to manage and monitor Information Systems.

B. Scope.

The scope of this procedure 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 procedure 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 procedure. In addition, the terms below apply for the limited purpose of this procedure.

A. Event – An observable occurrence in an Information System.

B. Information Security Office (ISO) – The University's information security department, which reports to the chief information security officer (CISO).

C. Log Management – The process for generating, transmitting, storing, protecting analyzing, retaining, and disposing of Log data.

D. Security Information and Event Management (SIEM) – Software that analyzes the data from different Log sources, correlates Events among the Log entries, identifies and prioritizes security Events, and initiates responses.

III. Procedure

A. All IT managers, IT Technicians, and Users managing Information Systems shall:

1. maintain a current and accurate inventory of all Assets for which they are responsible;
2. be knowledgeable of the applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations for the Information System and Information Asset Logs for which they are responsible;
3. document Log retention requirements;
4. enable logging for all Information Systems for which they are responsible;
5. secure and retain Logs in accordance with all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations;
6. configure Logs to be protected from unauthorized alteration, deletion, or changes;

7. as applicable, forward Logs based on consultation with the Information Security Office (ISO);
8. define “normal” Information System activity based on typical Information System use history;
9. configure alerting when Information System activity goes outside “normal” tolerances, including when an Information System fails to generate or forward Logs;
10. regularly review alerts to identify anomalies or suspicious behavior;
11. define appropriate processes to respond to alerts; and
12. immediately report any observed or suspected IT Security Incidents to the ISO.

    For more specific implementation requirements, please access Rule R4-004J.

B. IT managers shall:

1. provide support for all IT Technicians with Log Management responsibilities; and
2. establish Log Management responsibilities and expectations for IT Technicians.

C. The ISO shall, as applicable, provide consultation to IT managers, IT Technicians, and Users managing Information Systems for specific use cases and best practices.

Sections IV- VII are for user information about this procedure.

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

A. Policies/ Rules.

1. Policy 4-004: University Information Security Policy
2. Rule R4-004J: Log Management and Monitoring

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources.

1. IT Knowledge Base and Service Catalog

V. References

[*reserved*]

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 0.

1. Approved by Chief Information Security Officer with effective date of November 6, 2024.

B. Renumbering

1. Not applicable