WEBER STATE UNIVERSITY
Information Technology

Audit Log Management Standard (CIS CSC 8)

Purpose

Audit log management involves generating, storing, and analyzing log files to identify and respond to suspicious or anomalous events within WSU. Prioritizing and remediating vulnerabilities in WSU systems and software. The *Audit Log Management standard* outlines the processes and procedures for ensuring that logs are created and adequately analyzed. This standard applies to all departments and all assets connected to the WSU network.

Responsibility

Administrators are responsible for configuring the correct devices to generate, store, and transmit logs. All WSU assets are required to comply with the WSU audit logging procedures.

Exceptions

Exceptions to this standard may occur to accommodate unique circumstances. Exception requests must be made via email (security@weber.edu) and include the following information:

- The reason for the request,
- Risk to WSU of not following the written standard,
- Specific mitigations that will be implemented,
- Technical and other difficulties, and
- Date of review.

Audit Log Asset Lifecycle

This *Audit Log Management Standard* is divided into multiple sections based on asset usage patterns within WSU. The sections shown in Figure 1 are the high-level “steps” of the audit log management process, followed by detailed descriptions of each step.

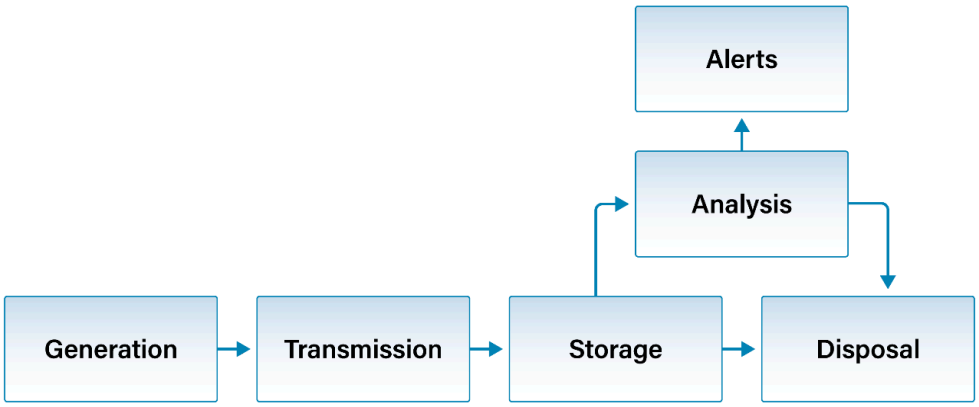

Figure 1. Audit Log Management Lifecycle

- **Generation** – Configuring assets to create audit logs.
- **Transmission** – Moving audit logs from local asset storage to a centralized datastore for collection and analysis.
- **Storage** – Securely storing and retaining audit logs for when analysis must be performed.
- **Analysis** – Analyzing logs to identify anomalous events and errors/issues with enterprise assets.
- **Disposal** – Removing or archiving audit logs from enterprise assets.

Generation

At Weber State University, all university-owned endpoints and central servers are protected by endpoint protection agents. These agents enable audit logging and log collection across covered assets. Configuration of audit log generation is centrally managed by the endpoint agents, preventing modification of audit log settings. Contractor assets and third-party service provider systems are outside the scope of this control. After operating system or software updates, log generation settings do not change as long as the endpoint agents remain operational.

Transmission

At Weber State University, logs from university-owned endpoints and central servers are sent to a central SIEM and log management platform. Log forwarding may occur in real time or on a scheduled basis, depending on the system.

Storage

At Weber State University, audit log retention is built into both the SIEM and local log management systems. Storage is maintained in both cloud and on-premises environments. Firewall rules restrict the transmission of audit data to approved audited systems only. Audit logs are encrypted at rest. Each audit storage system has its own defined retention period.

Analysis

At Weber State University, audit log analysis is performed through both automated and manual methods. Analysis is conducted using the central SIEM and custom solutions. Objectives include detecting security incidents, identifying vulnerabilities, troubleshooting issues, and correlating events across systems.

Disposal

At Weber State University, audit log retention and archival are determined by business needs and applicable regulatory requirements. Archived logs remain stored within the same systems used for active log management.

Alert

At Weber State University, audit log alerts are generated by the SIEM and via custom channels such as chat and email. Depending on the system and the nature of the alert, notifications are sent to various engineers within the IT Infrastructure, Operations, and Security department. Alerts undergo triage through automated logic or human analysis before further action is taken.

Generation

1. The contents of logs must be specified within the WSU CIS CSC 4_Secure Configuration of Enterprise Assets & Software Standard.
2. Audit logging must be enabled on all WSU assets where practical. WSU's endpoint management agents will enable the needed logging.
3. Audit logs must not be disabled on WSU assets.

Transmission

1. Logs from WSU assets are automatically collected and transmitted by the endpoint agent software or the log collector.
2. Access controls must be implemented to prevent unauthorized modification of audit logs.

Storage

1. Sufficient storage space must be allocated for audit logs for the duration required for analysis and retention.
    a. Sufficient space must be allocated to store audit logs on all relevant WSU assets.
    b. Sufficient space must be allocated for audit logs in any centralized audit log datastore.
2. Retention periods for audit logs should comply with the WSU CIS CSC 3: Data Management Procedure.

Review and Analysis

1. All high-severity events must be acted upon in accordance with the Information Security Office's incident response plan.

Disposal

1. All audit logs must be retained for the period specified by the audit log management process.
2. Archived logs must be available for analysis.
3. Disposal of audit logs should comply with the WSU CIS CSC 3: Data Management Procedure.

Revision History
Creation Date: February 24, 2026
Amended: N/A