SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **AUDIT LOG MANAGEMENT**	Procedure 8.23.01

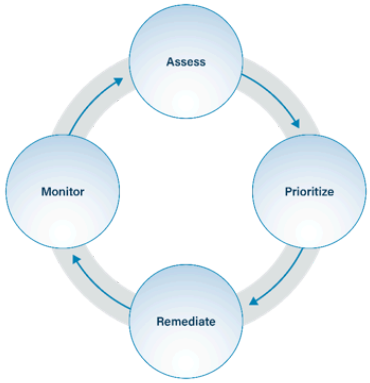
I. PROCEDURE STATEMENT

Audit log management includes generating, storing, analyzing logs files in order to identify and respond to suspicious or anomalous events occurring within the enterprise. Prioritizing and remediating vulnerabilities in enterprise systems and software. The *Audit Log Management Procedure* provides the processes and procedures for ensuring logs are created and properly analyzed. This policy applies to all departments and all assets connected to the enterprise network.

II. RESPONSIBILITY

The Information Technology ("IT") division is responsible for all log management functions. Specifically, administrators are responsible for configuring the correct devices to generate, store, and transmit logs. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems. All enterprise assets are required to comply with the enterprise audit logging procedures.

III. AUDIT LOG ASSET 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.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **AUDIT LOG MANAGEMENT**	Procedure 8.23.01

IV. GENERATION

A. An enterprise-wide strategy must be developed to establish and maintain an audit log process.
    1. This strategy must be documented.
    2. Documentation must be updated annually, or when significant changes have occurred.
    3. The contents of logs must be specified within the Secure Configuration Policy.
B. Audit logging must be enabled on all enterprise assets, as is practical.
C. Audit logs must not be disabled on enterprise assets.

V. TRANSMISSION

A. Procedures must be developed to move logs from enterprise assets to an audit log datastore.
    1. This may be done manually or via electronic means.
B. Access controls must be used to prevent audit logs from being modified in an unauthorized manner.

VI. STORAGE

A. Procedures must be developed to collect audit logs from enterprise assets.
B. Sufficient storage space must be allocated for audit logs for the period of time required for analysis and retention.
    1. Sufficient space must be allocated to store audit logs on all enterprise assets.
    2. Sufficient space must be allocated to store audit logs on any centralized audit log datastore.
C. Retention timeframes for audit logs should be in accordance with the enterprise data management process.

VII. REVIEW AND ANALYSIS

A. All high severity events must be acted upon in accordance with the audit log management process.

VIII. DISPOSAL

A. All audit logs must be stored for a period of a 90-day minimum (CIS Control 8).
B. Archived logs must be available for analysis.
C. Disposal of audit logs should be in accordance with the enterprise data management process.

LEGAL REFERENCES:

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, 8 (Audit Log Management)

- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Adopted: September 2025

Revised: N/A