Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-06
Subject:	IT Audit Log Management
Date Approved	February 21, 2024
Policy Owner's Title	Chief Information Security Officer
Policy Officer's Title	Deputy Superintendent of Operations
References: NIST Special Publication 800-53 Rev. 5 NIST Special Publication 800-92 -Center for Internet Security (CIS) Critical Security Controls – Control 8	

1) Purpose and Scope

a) The Purpose of log management is to collect, review and retain logs for the detection of Information Technology (IT) security incidents.
b) The scope of this document includes all Utah State Board of Education (USBE) systems.

2) Policy

a) Event Logging
    i) Audit log collection should include, but is not limited to:
        (1) Domain Name System (DNS) Query Audit Logs.
        (2) Uniform Resource Locator (URL) Request Audit Logs.
        (3) Command-Line Audit Logs.
    ii) Time Stamps
        (1) Internal system clocks should be used in the generation of time stamps for audit records.
            (a) At least two synchronized time sources across enterprise assets should be used to standardize time synchronization.
        (2) Time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.
b) Contents of Audit Log Records
    i) Configure detailed audit logging for enterprise assets containing sensitive data.
    ii) Audit Logs should contain information that establishes the following:
        (1) What type of event occurred.
        (2) When the event occurred.
            (a) Date and time of log on and log off, and other key events.
        (3) Where the event occurred.
            (a) Files and networks accessed.
        (4) Source of the event.
        (5) Outcome of the event.
            (a) Successful and failed attempts to access systems, data or applications.
            (b) Use of system utilities.
            (c) Exceptions and other security-related events, such as alarms triggered.

(d) Activation of protection systems, such as intrusion detection systems and antimalware.

(6) Identity of any individuals, subjects, or objects/entities associated with the event.

(a) User IDs.

(b) Terminal identity.

c) Audit Retention and Storage

i) The storage destination for audit logging must maintain adequate storage to comply with the enterprises Audit log requirements.

(1) The information system should provide a warning to Information Technology (IT) Operations when allocated audit record storage volume reaches 75% of repository maximum storage capacity.

ii) Consolidated collection and retention of audit log should be used where available.

iii) Audit logs across enterprise assets should be retained for a minimum of 90 days, unless otherwise directed.

d) Audit Review

i) Audit logs should be reviewed for anomalies or abnormal events that could indicate a potential threat at least on a weekly basis.

e) Audit Processing Failures

i) In the event of an audit processing failure, the system should alert IT Operations.

ii) Audit processing failures include:

(1) software/hardware errors,

(2) Failures in the audit capturing mechanisms,

(3) Audit storage capacity being reached or exceeded.

3) Change History

Date	Version	Author	Changes Made / Section(s)
October 6, 2022	0.1.0	Patrick Hawkins	Initial Draft