## GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exemptions or Exceptions
e. Policy Reviews and Updates

## SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all employees, contractors, and all other users of State information and information systems supporting the operation and assets of the State.

## AU-1 POLICY AND PROCEDURES

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls.

This document addresses the requirements set forth by the State to implement the family of Audit and Accountability security controls at the organization, process and/or system level for all information assets/State data.

The “AU” designator identified in each control represents the NIST-specified identifier for the Audit and Accountability control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capabilities that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an Executive Branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections in this document outline the Audit and Accountability requirements the State and Executive Branch agencies must implement and maintain to be compliant.

The State shall ensure information and information system audits are performed to account for, respond to, and minimize the impact of incidents on State information or systems.

This policy and associated procedures shall be reviewed and updated at least annually, or as State-defined events require.

## AU-2 EVENT LOGGING

An audit event is any occurrence in an information system significant and relevant to the security of those systems and their associated operating environments. The State and Executive Branch agencies shall detect these events to protect the integrity and availability of information systems by monitoring operational audit logs and:

a. Implement continuous monitoring and auditing of systems for unauthorized activity.
b. All network components and information systems must have the audit mechanism enabled and record logs of specified audit events.
c. Information systems logs containing Sensitive or Confidential data shall be audited at the operating system, software, and database levels.
d. A current, reliable baseline shall be established to audit for abnormalities.
e. Server, desktop, and laptop computers shall audit for the following events:
    i. Server startup and shutdown;
    ii. Starting and stopping of audit functions;
    iii. Loading and unloading of services;
    iv. Installation and removal of software;
    v. System alerts and error messages;
    vi. Application alerts and error messages;
    vii. Modifications to the application;
    viii. User logon and logoff;
    ix. System administration activities;
    x. Accesses to information, files, and systems;
    xi. Account creation, modification, or deletion;
    xii. Password changes;
    xiii. Modifications of access controls, such as change of file or user permissions or privileges;
    xiv. Any system owner-defined security related events relevant to that system;
    xv. Audit log file purge;
    xvi. Remote access outside of the State network communication channels;
    xvii. Changes made to an application or database by a batch file;
    xviii. Application-critical record changes;
    xix. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); and
    xx. All system and data interactions concerning federal tax information (FTI).
f. Network devices shall be configured to audit for:
    i. Device startup and shutdown;
    ii. Administrator (e.g., privileged user) logon and logoff;
    iii. Configuration changes;
    iv. Account creation, modification, or deletion;
    v. Modifications of privileges and access controls; and
    vi. System alerts and error messages

Audited events shall be reviewed and updated at least annually or when a major change to the information system occurs.

### AU-3 CONTENT OF AUDIT RECORDS

Information systems shall be configured to generate audit records containing sufficient information to determine:

a. Event date and time.
b. Software/hardware component of the information system where the event occurred.
c. Source and destination network addresses.
d. Source and destination port or protocol identifiers.
e. Event type.
f. Subject identity (e.g., user, device, process context).
g. Event outcome (i.e., success or failure).
h. Security-relevant actions associated with processing.

### AU-3 (1) CONTENT OF AUDIT RECORDS – ADDITIONAL AUDIT INFORMATION

System Owners and Business Owners, in coordination for system residing off State infrastructure, shall ensure service providers configure information systems to generate audit records containing the:

a. Manufacturer-specific event name / type of event
b. Full text recording of privileged commands
c. Individual identities of group account users

### AU-4 AUDIT LOG STORAGE CAPACITY

Audit record storage capacity must be allocated to retain audit records for the required audit retention period of three years per the requirement stated in the State's General Schedule for State Agency Records. This is to provide support for after-the-fact investigations of security incidents and to meet regulatory and State information retention schedule requirements.

a. Processing and storage capacity requirements shall be sufficient to capture and store the events cited above without adversely impacting operations.
b. On-line audit logs shall be backed-up to protected media well before the on-line logs reach storage capacity to prevent audit information being lost or overwritten.
c. For information systems containing FTI, sufficient audit record storage capacity must be allocated to retain audit records for the required audit retention period of seven (7) years.

### AU-5 REPONSE TO AUDIT LOGGING PROCESS FAILURES

The following requirements shall be met if an audit processing failure occurs:

a. Alerts must be immediately sent to State defined personnel or roles.
b. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall identify system process failures and provide information for corrective actions to be taken by the system administrator.
c. The system should automatically alert designated officials in the event of an audit failure or when audit capacity is 70%, 80%, and again at 90% utilization. This alert should be automated for system administrators to receive it after hours (e.g., email, text message).
d. Once the maximum storage capacity for audit logs is reached or there is an audit failure, the

information system should overwrite the oldest audit records or automatically shut down to eliminate the chance of an incident, in the absence of auditing and accountability.

### AU-5 (1) STORAGE WARNING CAPACITY

The system shall provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.

### AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Unauthorized activity shall be detected by monitoring operational audit logs to protect the integrity and availability of information systems.

a. State or agency-identified personnel shall review operational audit logs, including system, application, and user event logs for abnormalities.
b. Abnormalities and/or discrepancies between the logs and baseline shall be reported to agency management.
c. Access to audit logs shall be restricted to only authorized viewers, and the logs shall be protected from unauthorized modifications. File-integrity monitoring or change-detection software shall be used where feasible.
d. Review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized activity.
e. For systems containing FTI, refer to Section 4.3, Audit and Accountability, in IRS Publication 1075.

### AU-6 (1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING – AUTOMATED PROCESS INTEGRATION

Automated mechanisms shall be employed to integrate audit review, analysis, and reporting processes to support agency processes for investigation and response to suspicious activities.

Incident response, continuous monitoring, contingency planning, and State audit are some organizational processes benefiting from integrated audit review, analysis, and reporting.

### AU-6 (3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING – CORRELATE AUDIT RECORD REPOSITORIES

Audit records shall be analyzed and correlated across different repositories to gain organizational-wide situational awareness. Organizational-wide situational awareness includes awareness across all three tiers of risk management (e.g., organizational, mission/business process, and information system) and supports cross-organization awareness.

### AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

Audit reduction and report generation capability shall be provided and implemented to:

a. Support on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.
b. Does not alter the original content or time ordering of audit records.

## AU-7 (1) AUDIT RECORD REDUCTION AND REPORT GENERATION – AUTOMATIC PROCESSING

a. Information systems shall provide the capability to process audit records for events of interest based on AU-2. Events of interest can be identified by the content of specific audit record fields.
b. Audit event criteria may be defined to any degree of granularity required.

## AU-8 TIME STAMPS

Internal system clocks shall generate time stamps for audit records and that meet the State's Office of Information Technology (OIT) defined time synchronization and source; and that use either Coordinated Universal Time or include the local time offset as part of the time stamp.

## AU-9 PROTECTION OF AUDIT INFORMATION

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

a. Audit information and audit logging tools shall be protected from unauthorized access, modification, and deletion; and
b. State or agency-defined personnel shall be alerted upon detection of unauthorized access, modification, or deletion of audit information.

Protection controls include but are not limited to the control enhancements of AU-9 below:

## AU-9 (4) PROTECTION OF AUDIT INFORMATION – ACCESS BY SUBSET OF PRIVILEGED USERS

Access to management of audit functionality shall be authorized to an organizational-defined subset of privileged users. Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records.

## AU-11 AUDIT RECORD RETENTION

a. Information systems subject to IRS and SSA audits shall have their audit records retained for seven (7) years per Alabama Archives and History Records Disposition Authority and IRS Publication 1075 requirements.
b. Audit records associated with known incidents must be maintained in accordance with the State's record retention schedule after the incident is closed.
c. Agencies shall dispose of audit records when the retention time has expired, in accordance with the State's or IRS (for FTI information systems) record retention schedule after an incident is

closed.

## AU-12 AUDIT RECORD GENERATION

The State shall have the ability to generate audit records to monitor information systems use by employee and third-party contractor users. The following shall be done:

a. The information system must provide audit record generation capability for the list of events to be logged as defined in AU-2. Designated personnel can select which auditable events are to be audited by specific components of the system and generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.
b. Information systems shall be configured to provide audit record generation capability for the list of auditable events defined in AU-2 with content prescribed in AU-3 on the following information system components:
    i. Server, desktop, and laptop computers (file and print, web, firewalls, end-user environment)
    ii. Network components (e.g., switches, routers wireless)

## POLICY OWNER

Secretary of Office of Information Technology (OIT)

## MATERIAL SUPERSEDED

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

## REVISION HISTORY

| Revision Date | Summary of Change |
|---|---|
| 12/312024 | Policy Update |

**REMAINDER OF PAGE LEFT INTENTIONALLY BLANK**

## APPROVED BY

| | |
|---|---|
| Signature | Daniel Urquhart |
| Approved by | Daniel Urquhart |
| Title | Secretary of Office of Information Technology (OIT) |
| Date Approved | 01/15/2025 |

**REMAINDER OF PAGE LEFT INTENTIONALLY BLANK**