



KAY IVEY
Governor

STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



MARTY REDDEN
Secretary

POLICY 645: Audit and Accountability

| | |
|---------------------|---|
| VERSION NUMBER | Policy 645-01 |
| VERSION DATE | July 9, 2020 |
| POLICY TITLE | Audit and Accountability |
| OBJECTIVE | Information system event logging is an essential best practice for security and compliance. The objective of this policy is to define how agencies create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. |
| AUTHORITY | <p>The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of IT by state agencies, and exceptions to such authority, are derived from:</p> <p><i>Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).</i></p> |
| APPLICABILITY | The requirements and responsibilities defined in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as agency or agencies) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of state IT. |
| STATEMENT OF POLICY | Agencies must identify auditable events and audit processes sufficient to facilitate identification of root causes to problems and related events across various information systems and network devices operating within the state network architecture. |

It is the policy of OIT that:

- a) Information systems and network devices shall be capable of generating audit records for the auditable events deemed critical by agency executive management, by OIT, and by applicable federal laws, state laws, directives, policies, or standards. [AU-12]
- b) Executive branch agencies currently using a Security Incident and Event Management (SIEM) tool, shall send SIEM logs (by agreement) to the state Security Operations Center (SOC) SIEM instance. In addition to SIEM system logs, agencies shall forward SIEM alerts indicating abnormal network or user activity. [AU-2b.] [AU-6 (3)]
- c) Any agency that does not currently have a SIEM shall forward logs from other security products or servers to the state SOC. [AU-2b.]
- d) Audit records shall contain information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. [AU-3]
- e) Information systems and network devices shall be configured to send alerts to system administrators in the event of an audit event processing failure. Additional actions (e.g., shut down information system, suspend generation of audit records, etc.) shall be considered to restore audit processing capability. [AU-5]

OIT RESPONSIBILITIES

OIT shall:

- O.1 Coordinate security audit functions with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events. [AU-2b.]
- O.2 Establish baseline logging for events to be included in audit logs from information system including the content of audit records. [AU-3]
- O.3 Establish an audit log review schedule and reporting procedures. [AU-6]
- O.4 Configure automated network management software to support on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. [AU-7]

O.5 Provide an enterprise-wide authoritative time source synchronized to an external source (e.g., NIST, Naval Observatory). [AU-8]

AGENCY RESPONSIBILITIES

Agency system administrators shall:

A.1 Develop, document, and disseminate procedures facilitating the implementation of this audit and accountability policy, standards (i.e., audit requirements), and associated security controls. [AU-1a.2.]

A.2 Review and update agency audit and accountability policies at least once every three years and audit and accountability procedures at least annually. [AU-1b.]

A.3 Determine auditable events. [AU-2d.]

A.4 Provide rationale on why auditable events are critical to support investigations of security incidents. [AU-2c.]

A.5 Review and analyze information system audit records for indicators of inappropriate or unusual activity on state information systems or network. [AU-6a.]

A.6 Report adverse or suspicious findings to the Senior Agency Information Security Officer (SAISO) or Chief Information Security Officer (CISO). [AU-6b.]

A.7 Comply with the audit requirements defined by OIT, defined by the agency, or defined in security standards issued by federal agencies or other regulatory entities.

SUPPORTING DOCUMENTS

The following documents support this policy:

- [Standard 645S1: Audit Requirements](#)

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this policy and may aid in its implementation:

- NIST SP 800-53R4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-100: Information Security Handbook: A Guide for Managers

EFFECTIVE DATE

This policy shall be effective upon its approval by the Secretary of Information Technology as evidenced by the signature of the Secretary being affixed hereto.

The undersigned, as Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this policy to be adopted as of the date indicated below.

Marty Redden
Secretary of Information Technology

This _____ day of _____, 2020.

DOCUMENT CHANGE HISTORY

| Version | Version Date | Comments |
|---------|--------------|--|
| 645-01 | 07/09/2020 | Initial version (draft); supersedes Policy 677: Log Management |
| | | |
| | | |