SOUTH CAROLINA
DEPARTMENT OF EDUCATION

TITLE OF POLICY: SC Audit and Accountability Policy

SECTION: Information Security and Privacy

SUBSECTION: IT Compliance

POLICY NUMBER: 706.3

OFFICE OF RESPONSIBILITY: CISO

EFFECTIVE DATE: May 01, 2025

THE RELEVANT DEPARTMENT OF ADMINISTRATION POLICY IS ATTACHED. BELOW IS A SYNOPSIS OF THE POLICY CONTENTS:

1. Purpose and Scope

This policy is part of the South Carolina statewide information security framework and establishes requirements for audit mechanisms that support the monitoring, analysis, investigation, and reporting of security-related events across agency systems.

It applies to all state agencies and complements (but does not replace) other regulatory or legal requirements. Agencies are encouraged to tailor implementation to their operational needs while maintaining compliance with baseline standards.

2. Core Objective

The policy's central goal is to ensure that agencies maintain effective audit logging and accountability controls to:

- Detect inappropriate or suspicious activity
- Support incident investigation
- Maintain system accountability
- Strengthen overall security posture

3. Key Policy Requirements

A. Governance and Oversight (AU-1)

- Agencies must develop, document, and maintain audit and accountability policies and procedures.
- A designated official must oversee policy implementation and updates.
- Policies must align with applicable laws, regulations, and standards.

B. Event Logging (AU-2)

- Agencies must define what events are logged, how often, and why.
- Logging must support investigations and be reviewed regularly.
- Event selection should be coordinated across stakeholders.

C. Audit Record Content (AU-3)

Audit records must capture sufficient detail to reconstruct events, including:

- Event type, time, and location
- Source and outcome
- Associated users or entities

D. Log Storage and Management (AU-4)

- Agencies must ensure adequate storage capacity for audit logs.
- Logs should be transferred to alternate storage to preserve integrity and availability.

E. Failure Handling (AU-5)

- Systems must alert personnel when logging failures occur.
- Agencies must define and execute appropriate response actions.

F. Monitoring and Reporting (AU-6)

- Audit logs must be reviewed and analyzed for unusual or suspicious activity.
- Findings must be reported to appropriate personnel.
- Monitoring intensity should adjust based on changing risk conditions.

G. Time Synchronization (AU-8)

- Systems must use consistent, standardized timestamps (e.g., UTC or defined offsets).
- Time data must meet a defined level of precision for auditing.

H. Protection of Audit Data (AU-9)

- Audit logs and tools must be protected from unauthorized access, alteration, or deletion.
- Only authorized personnel may manage logging functions.
- Security alerts are required for unauthorized activity.

I. Retention (AU-11)

- Audit records must be retained according to records retention policies to support investigations and compliance requirements.

J. Audit Record Generation (AU-12)

- Systems must be capable of generating audit logs for defined events.
- Authorized personnel must be able to configure what is logged.
- Logs must include required content for effective auditing.

4. Security and Compliance

- Must comply with FERPA, state privacy laws, and the South Carolina Public Records Act.
- Content may be considered public record and is subject to audit or disclosure.
- This policy will be reviewed annually. Violations may result in disciplinary action or loss of access.

5. Related Policies

- SC Risk Assessment Policy (701.3)
- SC Access Control Policy (702.4)
- SC Personally Identifiable Information Processing and Transparency (704.1)

Information Security and Privacy Policy – Audit and Accountability

Division of Information Security

May 01, 2025

Revision History

Version Number	Date	Author(s)	Description
2.0	May 1, 2025	Division of Information Security	Updated for SCDIS-200 v2.0

CONTENTS

1.0 INTRODUCTION

A. Purpose

The South Carolina Statewide Information Security Program (SC Infosec Program) consists of information security policies, standards and guidelines that establish a baseline information security framework to protect the information technology systems of South Carolina state government agencies[1].

Implementing the baseline framework is critical to the development of an agency information security and privacy program. An effective information security and privacy program continually improves the overall security posture for the state, as it integrates and matures toward support of the state and organizational mission, goals and objectives.

This *Audit and Accountability Policy* establishes the requirements for audit mechanisms to enable monitoring, analysis, investigation and reporting of security-related events.

B. Authority and Responsibilities

The organizational and functional responsibilities for the South Carolina Division of Information Security (DIS) and Agency are established in the SC Infosec Program's "Master Policy."

C. Scope

Organizations shall comply with the SC Infosec Program's policies, standards and guidelines. Implementation of the SC Infosec Program's policies, standards and guidelines is not meant or intended to replace, supersede or otherwise nullify agency compliance requirements identified in other applicable federal, state, local, agency or institutional regulations, policies or guidance. Likewise, compliance with the SC Infosec Program's policies, standards and guidelines does not convey compliance with other regulatory requirements agencies may have for information security.

Organizations may implement policies, standards and guidelines "as-is," but are encouraged to develop additional agency or institution-specific guidance to address unique components of their business operations.

[1] The term "Agency" will be used to refer to SC state government agencies as described in the SC Infosec Program's "Master Policy."

2.0 AUDIT AND ACCOUNTABILITY POLICY STATEMENTS

A. Policy and Procedures [AU-1]

NIST CSF Reference: GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03

1. Agencies shall develop, document and disseminate:
    a. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines.
    b. Procedures to facilitate the implementation of the *Audit and Accountability Policy* and the associated audit and accountability controls.
2. Agencies shall designate an official to manage the development, documentation and dissemination of the audit and accountability policy and procedures.
3. Agencies shall review and update the current audit and accountability policy and procedures at defined frequencies and following defined events.

B. Event Logging [AU-2]

NIST CSF Reference: PR.PS-04

1. Agencies shall identify the types of events the system is capable of logging in support of the audit function.
2. Agencies shall coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.
3. Agencies shall specify the event types for logging within the system along with the frequency of (or situation requiring) logging for each identified event type.
4. Agencies shall provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
5. Agencies shall review and update the event types selected for logging.

C. Content of Audit Records [AU-3]

NIST CSF Reference: PR.PS-04

Agencies shall ensure audit records contain information that establishes the following:

1. What type of event occurred.
2. When the event occurred.
3. Where the event occurred.

4. Source of the event.
5. Outcome of the event.
6. Identity of any individuals, subjects or objects/entities associated with the event.

D. Audit Log Storage Capacity [AU-4]

NIST CSF Reference: None

1. Audit Log Storage Capacity [AU-4]:

   Agencies shall allocate audit log storage capacity to accommodate audit log retention requirements.

2. Transfer to Alternate Storage [AU-4 (1)]:

   Agencies shall transfer audit logs to a different system, system component or media other than the system or system component conducting the logging.

E. Response to Audit Logging Process Failures [AU-5]

NIST CSF Reference: None

1. Agencies shall alert designated personnel or roles in the event of an audit logging process failure.
2. Agencies shall take defined additional actions.

F. Audit Record Review, Analysis and Reporting [AU-6]

NIST CSF Reference: PR.PS-04, DE.AE-02, DE.AE-03

1. Agencies shall review and analyze system audit records for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
2. Agencies shall report findings to designated personnel or roles.
3. Agencies shall adjust the level of audit record review, analysis and reporting within the system when there is a change in risk based on law enforcement information, intelligence information or other credible sources of information.

G. Time Stamps [AU-8]

NIST CSF Reference: None

1. Agencies shall use internal system clocks to generate time stamps for audit records.
2. Agencies shall record time stamps for audit records meeting defined granularity of time measurement and use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or include the local time offset as part of the time stamp.

H. Protection of Audit Information [AU-9]

NIST CSF Reference: PR.DS-10

1. Protection of Audit Information [AU-9]
   a. Agencies shall protect audit information and audit logging tools from unauthorized access, modification and deletion.
   b. Agencies shall alert designated personnel or roles upon detection of unauthorized access, modification or deletion of audit information.
2. Access by Subset of Privileged Users [AU-9 (4)]:

   Agencies shall authorize access to management of audit logging functionality.

I. Audit Record Retention [AU-11]

NIST CSF Reference: PR.PS-04

Agencies shall retain audit records for a time period consistent with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

J. Audit Record Generation [AU-12]

NIST CSF Reference: PR.PS-04, DE.CM-01, DE.CM-03, DE.CM-09

1. Agencies shall provide audit record generation capability for the event types the system is capable of auditing.
2. Agencies shall allow designated personnel or roles to select the event types to be logged by specific components of the system.
3. Agencies shall generate audit records for defined event types that include defined audit record content.