	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 1 of 10

Scope


The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State’s distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

This policy document provides the State of North Carolina’s (State) security policy statements and commitment to develop, implement, and maintain an Information Security Audit and Accountability Policy and procedures to protect information and critical resources from a wide range of threats in order to ensure business continuity, minimize business risk for information systems and data of which the State is considered the owner.

Responsibilities

All covered personnel that utilize IT resources are responsible for adhering to this policy and any local Audit and Accountability requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for the continued development, implementation, and maintenance of information security policies, procedures, security controls and control techniques to address system security planning. Ensures that personnel with significant responsibilities for system audit requirements are trained.
Information System Owner	The Information System Owner is the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. Develops and maintains system audit and accountability process requirements in coordination with information owners, the system administrator, the information system security officer, and functional “end users.”
Information Owner	The Information Owner is the individual with operational responsibility and authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Provides input to information system owners regarding security requirements and security controls for the information system(s) where the information resides. Decides who has access to the information system and with what types of privileges or access rights. Assists in the identification and

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 2 of 10

	assessment of the common security controls where the information resides.
Covered Personnel	Covered personnel are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to enable the timely audit of system activities to reduce the risk of compromise of information or information systems managed by the State.
Third Parties	Third party service providers must provide Information Security Audit capabilities that meet State requirements. Third parties are required to maintain system audit controls and are subject to periodic review of audit accountability controls by the State.

AU-1 - Security Audit and Accountability Policy and Procedures


This policy provides requirements for the audit and accountability process which is required to document, respond to, and minimize the impact of incidents that can impact information systems and data of which the State is considered the owner.

The State has adopted the Security Audit and Accountability principles established in NIST SP 800-53 Rev 4 "Audit Accountability" control guidelines as the official policy for this security domain. The "AU" designator identified in each procedure represents the NIST-specified identifier for the Audit and Accountability control family. The following subsections in this document outline the Audit Accountability requirements that each Agency must develop, or adhere to in order to be compliant with this policy. The objective of this policy is to assure that there is information and information system audits to account for, respond to, and minimize the impact of incidents that can impact the State's information or information systems. This policy shall be reviewed annually, at a minimum.


AU-2 - Audit Events

An audit event is any observable occurrence in an agency's information system that is significant and relevant to the security of information systems and the environments in which those systems operate. Agencies shall detect these events and protect the integrity and availability of information systems by monitoring operational audit logs.

- a. Agencies shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity.
- b. All network components and computer systems used for agency operations must have the audit mechanism enabled and shall include logs to record specified audit events.
- c. Audit logs for information systems containing Restricted and Highly restricted data must be audited at the operating system, software, and database levels.

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 3 of 10

- d. The agency shall establish a current, reliable baseline that can be compared to audit logs to determine whether any abnormalities are present.
- e. Agencies shall configure server, desktop and laptop computers to 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, such as windows “runas” or linux “su” use.
 - 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 (e.g., use of suid/guid, chown, su)
 - xiv. Additional security-related events, as required by the system owner or to support the nature of the supported business and applications
 - xv. Clearing of the audit log file
 - xvi. Remote access outside of the agency network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system
 - 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)
 - xx. All system and data interactions concerning federal tax information (FTI)
- f. Agencies shall configure network device (e.g., router, firewall, switch, wireless access point) to audit for the following events:
 - i. Device startup and shutdown

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 4 of 10

- ii. Administrator logon and logoff
- iii. Configuration changes
- iv. Account creation, modification, or deletion
- v. Modifications of privileges and access controls
- vi. System alerts and error messages

AU-2 (3) - Audit Events – Reviews and Updates (Moderate Control)


Agencies shall review and update the audited events annually or when a major change to the information system occurs. Over time, the events that agencies believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

AU-3 - Content of Audit Records

Information systems shall be configured to generate audit records containing sufficient information to establish 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. At a minimum, the following elements shall be identified within each audit record:

- a. Date and time when the event occurred
- 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. Type of event that occurred
- f. Subject identity (e.g., user, device, process context)
- g. The outcome (i.e., success or failure) of the event
- h. Security-relevant actions associated with processing

AU-3 (1) - Content of Audit Records - Additional Audit Information (Moderate Control)

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 5 of 10

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 following additional elements:

- 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 Storage Capacity


Agencies must allocate audit record storage capacity to retain audit records for the required audit retention period of three years per the G116 Audit Trails File requirement stated in the NC [Department of Natural and Cultural Resources](#) 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. Agencies shall ensure that processing and storage capacity requirements are sufficient to capture and store the events cited above without adversely impacting operations.
- b. Agencies shall also ensure that on-line audit logs are backed-up to protected media well before the on-line logs are filled to capacity so that no audit information is lost or overwritten.
- c. For information systems containing FTI, agencies must allocate audit record storage capacity to retain audit records for the required audit retention period of seven (7) years.

AU-5 - Response to Audit Processing Failures

In the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded:

- a. Alerts must be sent to agency 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 be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator.
- c. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.
- d. 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 sent by a mechanism that allows system administrators to receive it after hours (e.g., email, text message).

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 6 of 10

- e. 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-6 - Audit Review, Analysis, and Reporting


Agencies shall detect unauthorized activity and to protect the integrity and availability of information systems by monitoring operational audit logs.

- a. Agencies shall designate staff to regularly review operational audit logs, including system, application and user event logs, for abnormalities.
- b. Any abnormalities and/or discrepancies between the logs and the baseline that are discovered shall be reported to agency management.
- c. Access to audit logs shall be restricted to only those authorized to view them and the logs shall be protected from unauthorized modifications, and if possible, through the use of file-integrity monitoring or change-detection software.
- 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.
- e. For systems containing FTI, refer to Table 10 – Proactive Auditing Methods to Detect Unauthorized Access to FTI in IRS 1075.

AU-6 (1) - Audit Review, Analysis, and Reporting – Process Integration (Moderate Control)

Agencies shall employ automated mechanisms to integrate audit review, analysis, and reporting processes, for example security information and event management (SIEM), to support agency processes for investigation and response to suspicious activities. Agency processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and State Auditor audits.

AU-6 (3) - Audit Review, Analysis, and Reporting – Correlate Audit Repositories (Moderate Control)

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 7 of 10

Agencies shall analyze and correlate audit records across different repositories to gain agency-wide situational awareness. Agency-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness.

AU-7 - Audit Reduction and Report Generation


- a. Audit reduction and report generation capability shall be implemented that does the following:
 - i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents
 - ii. Does not alter the original content or time ordering of audit records.
- b. The agency information system 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 including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.
- c. Agencies may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.
- d. This control is optional for LOW risk information systems.

AU-8 - Time Stamps

Internal system clocks shall be used to generate time stamps for audit records that are mapped to either Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) or local time with an offset from UTC that meets a DIT defined time synchronization and source.

AU-8 (1) - Time Stamps – Synchronization with Authoritative Time Source (Moderate Control)

The agency information system shall synchronize internal information system clocks at an agency-defined frequency to a DIT-defined authoritative time source. This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 8 of 10

AU-9 - Protection of Audit Information

Agencies shall protect audit information and audit tools from unauthorized access, modification, and deletion. Protection controls include the following:

- a. Writing audit trails to hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R).
- b. Backing up audit records onto a physically different systems or system component than the system or component being audited.
- c. Writing audit files to a log server on the internal network and subsequently backing them up to a secure location.
- d. Using cryptographic mechanisms to protect the integrity of audit information and audit tools. Cryptographic mechanisms include, for example, signed hash functions using asymmetric cryptography which allows verification of the hash information.
- e. Enforcing dual authorization for movement and deletion of audit information for information systems containing Restricted and Highly Restricted data.


AU-9 (4) - Protection of Audit Information – Access by Subset of Privileged Users (Moderate Control)

The agency shall authorize access to management of audit functionality to an agency-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.

The agency must authorize access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries.

AU-10 - Non-repudiation (Optional)

This control is optional for LOW and MODERATE risk information systems.

	<h1 style="margin: 0;">Audit and Accountability Policy</h1>		Document No. SCIO-SEC-303-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 9 of 10

AU-11 - Audit Record Retention

- a. State information systems shall retain audit records for at least three years per the G116 Audit Trails File requirement stated in the NC [Department of Natural and Cultural Resources](#) State's General Schedule for State Agency Records, Information Technology Records issued to provide support for after-the-fact investigations of security incidents and to meet regulatory and State information retention schedule requirements. For FTI, the agency must retain audit records for the events identified in AU-2 for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.
- b. Maintain audit records associated with known incidents, including those used for legal action, in accordance with the State's record retention schedule after the incident is closed.
- c. 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 the incident is closed.

AU-12 - Audit Generation

Agencies shall have the ability to generate audit records to monitor use of information systems by employee and third-party contractor users. Agencies shall do the following:

- a. The information system must provide audit record generation capability for the list of auditable events defined in AU-2. Designated State and agency personnel are allowed to 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, at a minimum, 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)

AU-13 – AU-16 (Optional)

These controls are not selected for LOW and MODERATE risk information systems.

