GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**532**	**Division:**	**Office of Information Technology**
Policy Title:	**Audit and Accountability (AU)**	**Effective Date:**	**January 17, 2025**
Version:	**3**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

To identify unauthorized access to the Agency's sensitive information. The purpose of this document is to establish procedures for the implementation of the Auditing and Accountability program that are authorized to operate within the sensitive information environment;

To ensure that the Agency's internal employees, subcontractors and vendors, and anyone with access to sensitive agency information is in compliance with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Audit and Accountability (AU) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Audit and Accountability (AU) requirements for DCH contractors, business owners, vendors, sponsors, and business partners regarding their roles and responsibilities when access to DCH data and use of applications associated with DCH operations is authorized; and

To reinforce the role of the business owner in providing adequate oversight of contractor responsibilities specific to Audit and Accountability (AU) obligations outlined in DCH contracts.

II. Scope

A. This document applies to all DCH personnel accessing or utilizing sensitive information in computer resources, data communication networks, or other information technology infrastructure resources owned or leased by DCH, including any other corporation or Agency with connectivity to the network, which is subject to these Information Security Policies.

B. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

C. Any personnel found to have violated any agency policy or process shall be subject to sanctions or disciplinary action, up to and including termination of employment.

III. Policy

A. Auditing and Accountability (AU) is the process of capturing and logging events and activities for the purpose of review, actions, investigations, resolutions, and subsequent retention.

B. The logging and capturing of significant events is vital to ensure that unauthorized activities, changes to system parameters, security and access changes, and modifications to critical data are captured and stored for retrieval when needed.

C. The auditing and monitoring activities are also vital to ensure that alerts are provided when significant events occur, and any such events are identified during the monitoring phase.

D. The monitoring of audit logs, in turn, determines which events or activities would need follow-up research to determine if an incident occurred.

E. Further, audit logs are required to be stored in a secured location to ensure that such files are needed in the event of audits, incident or event research, or legal issues.

F. The Audit and Accountability policy shall be reviewed annually to ensure its continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy shall be updated to reflect changes in relevant factors, such as technology, regulations, or internal practices. The revised policy shall be communicated to all affected parties.

G. In accordance with this policy, DCH shall:

1. The Chief Information Security Officer (CISO) shall be designated to manage the development, documentation, implementation, and dissemination of the Audit and Accountability (AU) policies and procedures.
2. Identify the type of audit events the organization can capture, specify the following event types for logging, and provide a rationale for doing so.
3. Shall ensure that, at a minimum, audit logs will capture the following fields:
    - What type of event occurred;
    - When the event occurred;
    - Where the event occurred;
    - Source of the event;
    - Outcome of the event;
    - Identity of any individuals, subjects, objects, or entities associated with the event; and
    - Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment.
4. Ensure that audit log storage capacity meets all records retention requirements.
    - Audit logs shall be securely kept in accordance with applicable legal and DCH policy record retention requirements.
    - Audit logs shall be stored in a different operating system than the system where the activity was logged.
5. Implement alerts to notify in case of an audit logging processing failure.
    - Provide an alternate audit logging capability in the event of a failure in the primary audit logging capability.
    - In the absence of alternative audit logging capability, invoke a shutdown or system degradation in the event of audit logging failures.
6. Logs shall be reviewed at least monthly to identify anomalies or unusual activity.
    - Adjust the logging and review parameters upon a change in risk or environmental updates.

- Link information from audit records with data obtained from monitoring physical access (or other non-technical sources) to identify suspicious, inappropriate, unusual, or malevolent activity.
- Specify all permitted activities for users, processes, and roles to help identify unauthorized activities.
- Conduct reviews of privileged users in a separate, dedicated repository from the system where the activity occurred, adhering to Separation of Duties (e.g., reviewer other than the user performing the action).

7. Support audit report generation capability and audit record reduction without compromising the ability to support historical, on-demand audit log reviews or the original audit log content including but not limited to the time and date stamp. Support the capability of logging the following events:
   - System resources;
   - Information objects accessed;
   - Identities of individuals;
   - Event types;
   - Event locations;
   - Event dates and times;
   - Internet Protocol addresses involved; and
   - Event success or failure.
8. Protect audit information and audit logging tools from unauthorized access, modifications, or deletions and alert the Office of Information Security (OIS) when such an event is detected.
   - Protect the integrity of the audit records and tools using cryptographic methods.
   - Restrict the access to managing the audit logging and the capabilities to be separate from those privileged users being audited. Restrict access to read-only.
9. Provide non-repudiation that an individual has irrefutably performed a logged action that could not be denied.
   - Maintain the chain of custody for information being reviewed and released.
10. Require that formal maintenance records are created, maintained, contain information, and are retained for at least seven years minimum as required by the Georgia Secretary of State Data Retention schedule.
11. Provide audit log generation for all security-relevant events and activities.
    - Ensure that system-wide time and date stamps are correlated to those time and date stamps from other devices or systems.
    - Produce audit records in a standardized format.
    - Provide the capability to perform user queries to retrieve data regarding an auditable activity.
12. Perform monitoring by the OIS to identify any unauthorized organizational information disclosures and notify the OIS for follow-up action**.**
13. Provide the capability for session audits that may include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers in accordance with applicable laws, regulations, directives, and policies.
    - Session audits should be initiated at start-up and have the capability of remote monitoring.

14. Support cross-organizational audit logging when audit information is transmitted between organizations.
15. Roles and Responsibilities:
    - Business Owners: Ensure that systems under their management adhere to audit requirements, including appropriate logging configurations and review processes.
    - System Administrators: Implement and maintain logging mechanisms per the Office of Information Security (OIS) guidance and ensure audit data integrity and security.
    - Contractors and Vendors: Comply with contractual obligations concerning audit and accountability measures, including participation in audits and incident investigations as required.
    - CISO: Approves audit configurations, ensures compliance with legal and regulatory frameworks, and manages overall accountability for the AU program.

IV. Definitions

- Auditing and Accountability (AU) - the process of capturing and logging events and activities for the purpose of review, actions, investigations, resolutions, and subsequent retention.
- Chain of Custody - the process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each individual who handled the evidence, the date and time the evidence was collected or transferred, the purpose for the transfer, and where the evidence was kept.
- DCH – Georgia Department of Community Health.
- ePHI - Electronic protected health information or ePHI is defined in HIPAA regulation as any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media. HIPAA regulation states that ePHI includes any of 18 distinct demographics that can be used to identify a patient. See 45 C.F.R. §§ 160.103 and 164.514(b)(2).
- FISMA – Federal Information Security Modernization Act.
- HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law requiring national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
- NIST – The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See https://www.nist.gov/.
- PII – Personally Identifiable Information - PII is defined by Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017). PII means information that can be used to distinguish or trace an individual's identity either alone, or when combined with other information that is linked or linkable to a specific individual.
- PHI – Protected Health Information – Individually identifiable health information that is:
    - Transmitted by electronic media
    - Maintained in electronic media; or

- Transmitted or maintained in any other form or medium.
- Excluding individually identifiable health information in:
  - Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
  - Records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
  - Employment records held by DCH (a covered entity) in its role as employer; and
  - Regarding a person who has been deceased for more than fifty (50) years.

- Sensitive Information - PII, PHI, ePHI, proprietary/trade secret and similar data that require special handling.

V. References: Please refer to NIST 800-53 Auditing and Accountability (AU) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for System and Information Integrity.

January 21, 2025

Signature ***Date***

Revision History

Version	Date	Description	Author
1.0	11/23/2023	Reviewed and Approved by DCH CIO; establishing v1.0	DCH CISO
2.0	11/4/2024	• Added a revision history table to validate consistent review/update and document changes • Section F: The Audit and Accountability Policy shall be reviewed annually • Section G.1: The Chief Information Security Officer (CISO) shall be designated to manage the development, documentation, implementation, and dissemination of the Audit and Accountability (AU) policies and procedures. • Section G.6: Logs shall be reviewed at least monthly • Section G.10: Require that formal maintenance records are retained for at least seven years minimum	DCH CISO
3.0	1/17/2025	• Added Section G.15: Roles and Responsibilities	DCH CISO