GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**531**	**Division:**	**Office of Information Technology**
Policy Title:	**Awareness and Training (AT)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

To properly protect sensitive information from losses due to the accidental or intentional misuse of information technology resources, personnel must be adequately trained in the principles of information security. This document provides guidance on creating a security awareness training program.

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 Awareness and Training (AT) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Awareness and Training (AT) 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 Awareness and Training (AT) obligations outlined in DCH contracts.

II. Scope

A. This document applies to all 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. DCH policy is to implement and manage a formal security awareness program. All personnel shall be adequately trained in information security principles, including the written security policies and procedures that must be followed. This policy requires that all personnel and contractors attend security awareness training upon hire, at least annually, and upon revision to compliance requirements. DCH shall maintain training records for all personnel and contractors.

B. DCH shall implement and disseminate policies and procedures to all personnel and contractors. Formal security and privacy awareness training sessions shall be developed and implemented. Training may be generated internally using best practices defined in NIST publications or contracted to a professional third-party provider. The Agency shall conduct an internal annual review of the effectiveness of the security and privacy training program as well as a review of the policies and procedures.
Before being granted access to state data, a contractor shall ensure that all staff, contractors, and other individuals requiring access to State data complete organizationally provided cybersecurity & HIPAA security awareness training and applicable training on protecting sensitive information. State service agreement requirements, applicable federal laws, regulations, and business associate agreement requirements should determine awareness training criteria. Contractors must ensure that all staff and subcontractors are trained before being allowed access to state data and undergo refresher training at least annually. Training records must be maintained and provided to the State upon request. Awareness training criteria should address the following subject areas, including but not limited to:

1. Role-based Access Control
2. Encryption of Stored and Transmitted sensitive information
3. HIPAA Omnibus Laws, Regulations, and Standards
4. Privacy & Security Incident Response Policy and Procedures
5. Sanctions for Violations of HIPAA Privacy and Security Policies
6. Privacy Act Legislation for the protection of PII
7. Cybersecurity Awareness Training

C. The Chief Information Security Officer shall be designated to manage developing, documenting, implementing, and disseminating the awareness training policy and procedures.

D. In accordance with this policy, DCH shall:

1. Provide privacy and security awareness training to information system users, including managers, senior executives, and contractors, as part of initial training for new users. Refresher training shall be provided at least annually and when required by information system changes or environmental or regulatory updates.
2. Include exercises and real-life simulations as part of the training curriculum and recognize and report on the potential indicators of insider threats.

3. Incorporate lessons learned from internal or external security incidents, disaster events, or breaches into literacy and role-based training and awareness techniques.
4. Provide role-based targeted security training to personnel with assigned security roles and responsibilities. Training shall be provided before authorizing access to the information system or performing assigned duties. Training recipients must receive a passing grade score to complete training modules successfully.
5. Provide refresher training at least annually and when required by information system changes. Lessons learned shall be incorporated into the process. DCH Cyber Security Office administers the new hire and annual training curriculum and updates the program as needed and/or annually.
6. Require personnel and contractors to acknowledge at least annually that they have read and understood the security policy and procedures.
7. Document and monitor information security and privacy training activities and maintain training records for a minimum period of 7 years**.**
8. Provide feedback on organizational training results to the Chief Information Security Officer to take appropriate action upon receiving feedback and adjust the training methodology as needed.
9. Provide periodic security updates and annual refresher courses to remind personnel about their obligations and responsibilities concerning sensitive information security.

E. Definitions

- 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 – The Federal Information Security Modernization Act of 2014.
- 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.
- Least Privilege (Minimum Necessary) – Granting the minimum access needed to perform a specific job role or function.
- 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.
- Role Based Access – Access Group or profile based on defined job functionality within a department or team.
- Sensitive Information - PII, PHI, ePHI, proprietary/trade secret and similar data that require special handling.

F. References: Please refer to NIST 800-53 Awareness and Training AT and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Awareness and Training.

November 23, 2023

Signature ***Date***