GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**543**	**Division:**	**Office of Information Technology**
Policy Title:	**Personnel Security (PS)**	**Effective Date:**	**November 08, 2024**
Version:	**2**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

The development, implementation, and administration of an overall Personnel Security (PS) program is critical to protect sensitive information from losses due to the accidental or intentional misuse of information technology resources. This document provides guidance on creating and maintaining this program.

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

To establish Personnel Security 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 Personnel Security 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. DCH's policy is to implement and manage a formal personnel security program that is reviewed and updated at least annually or when circumstances require additional review.

B. DCH shall implement and disseminate this policy and procedures to all personnel and contractors.

C. DCH shall designate the Chief Information Security Officer to manage the development, documentation, implementation, and dissemination of this Personnel Security policy and procedures in addition to managing the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Personnel Security policy and plan that addresses purpose, scope, roles, and procedures.
2. Develop and establish an Insider Threat Program that:
    - Identifies and assigns a risk designation to all positions in the company that determines high-risk insiders.
    - Established pre-employment screening (background checks) for all employees, contractors, and third-party providers (managing and accessing sensitive data) that is commensurate with risk designations.
    - Perform an annual review on DCH enterprise-wide risk designation.
3. Pre-screen personnel and contractors before allowing access to DCH systems.
    - Based on risk designation, there may be a need to re-screen current DCH personnel.
    - Verify that individuals accessing confidential systems have been authorized and approved to do so.
4. Establish the following controls to follow when personnel terminate from DCH.
    - Disable all system and physical access within **24 hours (and immediately for involuntary)** upon termination.
    - Retrieve all DCH property (e.g., tokens, badges. cell phones, keys, etc.) Utilize an exit checklist.
    - Conduct exit interviews with terminated personnel.
    - Retain access to all DCH information.
    - Notify terminated personnel of all binding confidentiality agreements regarding the continued protection of DCH information plus non-compete agreements as applicable and require them to acknowledge and sign their obligations.
    - Ensure that termination notifications are sent to the appropriate personnel within 24 hours.
5. The Personnel Security 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.
6. DCH shall ensure that personnel security requirements for third-party personnel are documented and integrated into contracts, Business Associate Agreements (BAAs), and other formal agreements. These documented requirements will specify the security clearances, background checks, access controls, and other security measures necessary to protect DCH assets and information. All third-party personnel will be required to acknowledge and comply with DCH's personnel security policies, including any relevant legal and regulatory compliance obligations.
7. Perform a review of both logical and physical access by the incoming manager within **30** days of transfer from one business unit or Agency to another,

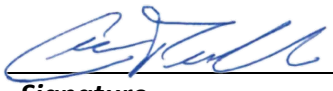
    - Based on feedback from the incoming manager, adjust/remove access within **30** days of access review.
8. Develop and implement access agreements that all personnel requesting access to DCH systems must sign.
    - Agreements should include acceptable use, rules of behavior, protection of confidential information, remote usage, non-disclosure provisions, and an acknowledgment that the signer understands and agrees to abide by the agreement.
    - Agreements should be reviewed and updated annually or upon changes in requirements or within the environment. When agreements are revised, a new agreement must be reviewed, acknowledged, and signed.
    - Agreements shall state that the provisions to protect DCH information are legally binding post-employment.
9. Identify and establish security requirements for external service providers.
    - Require state and agency service providers to abide by all DCH security requirements.
    - Require service providers to notify DCH of all personnel terminations or transfers with logical or physical access to DCH resources within a 24-hour.
    - Monitor service providers for performance and compliance.
10. Document and implement a formal sanctions program for individuals failing to comply (unintentionally or intentionally) with DCH policies, requirements, and procedures.
    - Notify the individual's manager upon receiving a complaint and initiating a sanction, identifying the involved individual and the reason.
11. Ensure that DCH security and privacy roles, responsibilities, and training requirements are documented and in place.

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 – 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.

F. References: Please refer to NIST 800-53 Personnel Security (PS) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Personnel Security.



11/11/2024

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	11/08/2024	• Added a revision history table to validate consistent review/update and document changes • Section D.4: Ensure that termination notifications are sent to the appropriate personnel within 24 hours • Section D.5: The Personnel Security Policy shall be reviewed annually • Section D.6: Personnel security requirements for third-party personnel	DCH CISO