GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**540**	**Division:**	**Office of Information Technology**
Policy Title:	**Physical and Environmental Protection (PE)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

To properly protect sensitive information from losses due to accidental or intentional misuse of information technology resources, the development, implementation and administration of an overall program management program is critical. 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 Physical and Environmental Protection (PE) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Physical and Environmental Protection (PE) 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 Physical and Environmental Protection (PE) 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 physical and environmental protection 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 Physical and Environmental Protection policy and procedures and manage the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Physical and Environmental Protection Policy and plan that addresses purpose, scope, roles, and procedures.
2. Identify, authorize, and maintain a list of individuals with access to the physical facilities where information systems reside based on their function or job role.
    - Issue identification badges, credentials, or passes for those authorized individuals.
    - Review the facility authorization access list at least on a yearly frequency to confirm access is still required.
    - Remove individuals from the authorized access list when access is no longer required (e.g., termination, transfer, short term visitor, etc.)
    - Require two forms of identification for visitors seeking access to the facility, with at least one being a picture identification.
    - Restrict unescorted access to the physical facilities where systems reside to those explicitly authorized.
3. Verify the individual's authorization before granting access to the facility.
    - Ensure that entrance and exit points to the facility are controlled via physical security staff at the Agency offices and data centers (e.g., wiring closets) and technical controls (e.g., badge readers).
    - Maintain and retain Physical Access Audit Logs for at least 3 months immediately available and up to a year archived.
    - Escort all visitors and monitor/control their on-site activities.
    - Secure keys and combinations and any physical security devices.
    - Change keys and combinations when devices are lost and compromised or following personnel termination/transfer.
    - Maintain an inventory and track the proliferation of all physical devices (e.g., locks, key card readers, combination locks, biometric readers, etc.
    - Establish and enforce separate physical access to the system (e.g., access to a secured computer room) and access to the facility.
    - Deploy guards as a 24x7 physical access control to the facility.
    - Use lockable (and locked) physical casings to protect DCH information resources.
    - Utilize physical barriers when possible (e.g., high cubicle walls, locks on offices, computers, building entrance barriers, etc.)
    - Use access vestibules to prevent piggybacking into a secured area.

4. Control physical access to system equipment and peripherals (e.g., physical jacks, servers, etc.)
5. Control physical access to output devices.
6. Require individuals to identify and authenticate before obtaining output (e.g., via their badge) for accountability and authorization.
7. Have a plan to respond to Physical Incidents and coordinate investigations with the Incident Response function.
8. Protect power equipment and cabling from damage and destruction (both natural occurrences (floods, fires, tornadoes) and unnatural occurrences (vandalism, sabotage, human error/accidents).
    - Deploy physically segregated and redundant power cabling.
    - Deploy automatic voltage controls (e.g., voltage regulators).
9. Ensure that emergency power shutoff capability exists, is known to authorized personnel, and is protected from unauthorized personnel.
10. Provide an alternate uninterruptable power supply to ensure minimal operations when the main supply is interrupted (e.g., generators).
    - Ensure that the power supply is self-contained and independent of primary and externally generated power supplies.
11. Implement and maintain emergency lighting to be deployed in the event of a power failure.
12. Maintain automated environmental controls that regulate temperature, humidity, water pressure, etc.
    - Provide alerts, alarms, or notifications when targeted levels are changed to a potentially harmful level to equipment or personnel.
13. Develop a process for authorizing, managing, and tracking system components and equipment entering and leaving the facility. Identify authorized ingress and egress points.
14. Secure system components by placing them in secured areas to minimize the likelihood of physical and environmental hazards as well as damage from unauthorized individuals.
15. Implement a methodology for inventorying, tracking, and monitoring critical assets and their movements (e.g., physical moves from one location to another, retiring an asset, new asset, etc.)

E. Definitions

- Access Vestibules - An empty space between 2 physical barriers requiring authentication.
- 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.
- Matching Program - a comparison of records from two or more automated systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof).
- 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.
- Physical Media – Hard copy documents, faxes, microfiche
- Sensitive Information - PII, PHI, ePHI, proprietary/trade secret and similar data that require special handling.

F. Please refer to NIST 800-53 Physical and Environmental Protection (PE) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Physical and Environmental Protection.

November 23, 2023

Signature ***Date***