GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**541**	**Division:**	**Office of Information Technology**
Policy Title:	**Planning (PL)**	**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 Planning (PL) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Planning (PL) 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 Planning (PL) 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 planning 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 (CISO) to manage the development, documentation, implementation, and dissemination of this planning 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 planning policy and plan that addresses purpose, scope, roles, and procedures.
2. Develop and implement an overall security and privacy plan that addresses the following:
    - Incorporate mission and business processes and account for all system components and system architecture.
    - Identify and record all types of information stored, processed, and transmitted by DCH systems and dependencies on other systems (e.g., downstream feed)
    - DCH shall categorize all PII and PHI with a data security categorization risk level of **MODERATE RISK** based on the NIST/FIPS 199 Data Security Categorization standard.
    - From the Risk Assessment and Business Impact Analysis note any likely and impactful threats to DCH systems. (Note: Risk Assessment plan will be addressed in the Risk Assessment (RA) plan and the Business Impact Analysis will be addressed in the Contingency Plan (CP).
    - Incorporate privacy concerns, personally identifiable information (PII), and Protected Health Information (PHI) into risk assessments.
    - Define minimum security and privacy controls in a system security plan based on NIST 800-53 (most current version) and submit it to DCH for review and approval. Document all identified control gaps and draft a plan of action to remediate identified gaps.
    - Independently assess security plans on an annual basis by a third-party accessor or by the vendor's third-party assessor and provide a Security Assessment Report (SAR) annually. Assessment may be performed more frequently than annually upon risk posture or architectural changes.
    - Identify and document baselines for each system and obtain plan approval from CISO. Deploy and review baselines on at least an annual basis. (Note: NIST 800-53 Moderate Control Set for each application Baselines are a minimum level of acceptable security controls based on regulatory and DCH requirements and organizational needs.
    - Document existing controls and implementation descriptions, compare to minimum security baselines and create an action plan to address identified gaps.
    - Ensure that minimum security baselines are met or exceeded on new planned systems and note any impacts to security and/or privacy before putting them into production.

    - Security plans and baselines shall be protected from unauthorized modification or disclosure and reviewed at least annually or as needed.
3. Ensure that rules of behavior are documented, disseminated, and remain current for personnel requiring system access.
    - Require users to acknowledge and sign that they understand and agree to abide by DCH security policies and requirements.
    - Review and update the rules of behavior (Acceptable Use Agreement) at least annually or as dictated by requirements and environmental changes. Upon change, re-require users to acknowledge and sign the amended document.
    - Rules of behavior shall govern the use of internet sites and social media (both using DCH resources and when accessing social media as a private individual).
4. Develop, document, and implement a Concept of Operations (CONOPS) describing how the system will be operated and comply with security and privacy requirements. The CONOPS document shall be reviewed and updated during the System Development Lifecycle (SDLC). DCH shall document the specifics of this CONOPS within each Information Systems Security Plan based on NIST-800-53 criteria.
5. Develop, document, and implement a security and privacy architecture plan that: (Note: Each NIST-800-53 Security Plan contains an architectural overview and a diagram of each.)
    - Describe the requirements and how organizational and private information shall be processed and protected from a confidentiality, integrity, and availability perspective and reviewed annually (or when conditions or environmental changes require further review).
    - Deploy multiple/layered security controls (e.g., multi-factor authentication).
    - Utilize a diversity of vendor provided products to enhance complementary capabilities (e.g., alerting, detection of malicious code, data exfiltration, etc.)
6. Implement enterprise wide controls and centrally manage/track the state of the controls. DCH requires that all applicable NIST-800-53 controls be described in detail regarding how they are implemented within the SSP.
7. Customize minimum security baselines by deploying common controls and additional controls to meet the requirements and needs of DCH.

E. Definitions

- CONOPS (Concept of Operations) – a document describing the characteristics of a system and how the system is intended to be used.
- 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.

- Minimum Security Baseline – minimum acceptable level of required controls in a system.
- 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.
- POAM (Plan of Action and Milestone Report) - Plan to remediate identified control gaps from the SAR. Remediation dates and milestones are defined into the plan and dates are tracked and reviewed to completion.
- SAR (Security Assessment Report) – Security control assessment results.
- SDLC (System Development Lifecycle) - system/software phases from conception to development to testing to acceptance, approval and implementation.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.
- SSP – System Security Plan that documents how an organization implements its security requirements and security guidelines and standards that the organization follows.

F. Please refer to NIST 800-53 Planning (PL) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Planning.

Signature

November 23, 2023

Date