GEORGIA DEPARTMENT OF COMMUNITY HEALTH			Enterprise Policy
Policy No.:	**542**	**Division:**	**Office of Information Technology**
Policy Title:	**Program Management (PM)**	**Effective Date:**	**December 17, 2025**
Version:	**3**	**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 Program Management (PM) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Program Management 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 Program Management 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 program management 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 program management policy and procedures, in addition to managing the program.

D. The Program Management policy and procedures shall be reviewed annually to ensure their continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy and/or procedures shall be updated to reflect changes in relevant factors, such as assessment or audit findings; security or privacy incidents; changes to applicable laws (including privacy laws); Executive Orders, directives, regulations, policies, standards, and guidelines. The revised policy and/or procedures shall be communicated to all affected parties. Evidence of this review, including formal sign-off sheets or meeting minutes from the Senior Official, shall be retained for audit purposes.

E. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Program Management policy and plan that addresses purpose, scope, roles, and procedures. This plan shall be protected from unauthorized disclosure and modification via role-based access controls (RBAC) within the DCH secure document repository, with read-only access for general staff and write access restricted to the CISO and designated policy owners.
2. Identify documents and budget all resources needed to implement and manage the security and privacy program in accordance with applicable laws, executive orders, directives, policies, regulations, and standards. DCH shall retain specific budgetary artifacts as assessable evidence that information security and privacy resources are explicitly included in capital planning cycles.
3. DCH (enterprise wide) shall develop and maintain a plan of action that includes milestones, target dates, remediation steps, management actions, and risk and impact analysis. The management of these items shall be governed by the 'DCH POA&M Standard Operating Procedure (SOP),' which defines the specific entry, validation, and closure steps within the ServiceNow IRM platform.
4. Ensure that the plan of action is tracked and reported per DCH reporting requirements.
5. Develop, maintain, and keep current an inventory of all operating systems, applications, and processes that store, process, or transmit personally all sensitive and confidential data, including identifiable information. DCH shall employ automated mechanisms, such as Data Loss Prevention (DLP) scanning tools, to continuously verify that PII has not migrated to un-inventoried systems and to reconcile data flows against the authorized inventory.
6. Develop and document a means to measure the security and privacy program performance via metrics reporting, dashboards, Service Level Agreements, etc. Specific organization-defined metrics (e.g., Mean Time to Remediate, Phishing Click Rate, Patch Compliance) shall be defined and maintained in the 'DCH Security Metrics Standard' and reported monthly.
7. Incorporate security and privacy requirements into the enterprise architecture program. Security reviews are mandatory during the architectural design phase for all new projects to ensure security safeguards are built in before development.
8. Exclude non-essential functions from the systems that support critical functions (e.g., printing, ordering supplies…)

9. Ensure that all aspects of critical infrastructure (e.g., development, documentation, updating/upgrading) address security and privacy concerns. These protections shall be documented in the 'DCH Critical Infrastructure and Key Resources Protection Plan,' which identifies critical assets and defines specific resilience strategies.
10. Develop, implement across the enterprise, and maintain a comprehensive risk management plan that manages security and privacy risks to operations, assets, individuals, and other organizations.
11. Review and update the risk management plan on at least an annual basis or when requirement and/or environmental changes occur.
12. Identify, document, and implement an enterprise-wide authorization process that:
13. Identifies and designates functions and individuals to fill the roles and responsibilities.
14. Incorporate the authorization process into the risk management program.
15. Define and document the organizational mission statement and business processes with consideration given to security and privacy concerns, potentially resulting in risk to DCH.
16. Based on the mission statement, identify information protection controls needed.
17. Review the mission statement and business processes as dictated by regulatory or environmental changes.
18. Develop and deploy a robust Insider Threat program that is integrated with the Incident Response Plan. This program shall be overseen by a designated Cross-Discipline Insider Threat Team (comprising representatives from Security, HR, and Legal) that meets at least quarterly to review insider risk indicators and coordinate response actions.
19. Establish a workforce development program for individuals assigned security and privacy roles.
20. Develop an oversight program to ensure that training, testing, and monitoring functions are implemented, performed, maintained, and aligned with risk management goals.
21. Develop and maintain contacts and exchange information with other security and privacy professionals and associations in external organizations for the purpose of;
22. Facilitating ongoing training and staying current with security and privacy best practices.
23. Sharing information on emerging threats and vulnerabilities.
24. Implement a threat awareness program to educate and defend against ongoing and emerging threats to the organization.
25. Utilize automated tools to detect and alert to the presence of threats.
26. Implement a process to ensure that non-confidential data is protected on external systems that store, process, or transmit such data.
27. Develop a mechanism to verify that the external providers' controls are implemented and functioning as designed.
28. Develop, implement, and disseminate the DCH Privacy Program plan that includes:
29. Mission statement, roles, responsibilities, requirements, controls, and how the program is structured.
30. Strategic goals of the program and management commitment to its success.
31. The relationship and coordination between the different DCH organizations in managing the privacy program.

32. Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, implement, and maintain applicable privacy requirements into an approved plan.
33. Review and update the plan at least annually or to address changes in federal privacy laws and policy, and organizational changes and problems identified during plan implementation or privacy control assessments.
34. Provide information about DCH's privacy program, practices, reports, and activities on a publicly accessible website.
35. Provide the means to communicate with senior DCH privacy officials as well as contact information via email addresses and phone numbers.
36. Develop and post privacy policies on the website.
37. Update and repost policies whenever DCH modifies the privacy practices.
38. Develop and implement a plan to maintain an accurate accounting of when Personally Identifiable Information (PII) is disclosed that includes the following:
39. Data, nature, and purpose of disclosure.
40. Name, address, or other contact information of the organization or individual to whom the information was disclosed.
41. Retained for a period of at least 7 years following the disclosure.
42. Upon request, make the accounting of the disclosure available to the impacted individual(s).
43. Develop, document, and implement enterprise-wide procedures for:
44. Reviewing the accuracy, timeliness, relevancy, and completeness of PII across the organization and correcting or deleting incorrect or obsolete data.
45. Providing a notice of corrected or deleted PII to individuals.
46. Handling appeals of adverse decisions regarding corrected or deleted data.
47. Establish a data governance body to ensure that data use (storage, processing, and transmission) aligns with privacy and security requirements.
48. Document and implement a process for receiving, responding to, and investigating complaints confidentially or general requests for security and privacy controls and practices.
49. Implement a mechanism to ensure that all received complaints are acknowledged and responded to promptly and tracked to resolution.
50. Define and implement a mechanism for privacy reporting.
51. Identify what needs to be reported and the target audience to disseminate reports.
52. Review and update reports and report structures at least periodically or upon changes to the environment or regulatory requirements.
53. Formally establish and identify the role/function responsible for implementing and managing the Risk Management Program (CISO).
54. The Risk Management role is responsible for identifying, reviewing, responding to, and managing risks across the DCH enterprise.
55. Develop and implement an enterprise-wide strategy for managing supply chain risks introduced by the development, acquisition, servicing, transfer, and disposal of systems and system components.
56. Identify and document all suppliers of critical products and services.
57. Develop and implement an enterprise-wide monitoring program that:
58. That monitors for DCH defined metrics.

59. Establishes a process and frequency for monitoring and assessing control effectiveness.
60. Implements a process for analyzing and responding to results of monitoring and assessing control effectiveness.
61. Develop and implement an enterprise-wide process to analyze and ensure that system resources are being utilized in alignment with their intended purposes.

F. 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.
- 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.

- Plan of Action and Milestones (POA&M) – A document that identifies tasks needing to be accomplished to remediate security weaknesses. It details resources required, milestones, and scheduled completion dates.
    - Sensitive Information - PII, PHI, ePHI, proprietary/trade secret and similar data that require special handling.

G. Please refer to NIST 800-53 Project Management (PM) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Program Management.

12/18/2025

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	11/21/2024	• Added a revision history table to validate consistent review/update and document changes • Section D: The policy shall be reviewed annually	DCH CISO
3.0	12/17/2024	• Section III.D: Updated to require retention of formal evidence (sign-offs or meeting minutes) for the annual policy review and to explicitly reference "policy and procedures" to clarify the full scope of requirements. Added specific definitions for factors that influence the policy and procedures revision process. • Section III.E.1: Mandated role-based access controls (RBAC) to protect the Program Management plan within the secure document repository. • Section III.E.2: Added requirement to retain budgetary artifacts as evidence of security resource inclusion in capital planning. • Section III.E.3: Formalized the use of the POA&M Standard Operating Procedure and ServiceNow IRM for managing remediation actions. • Section III.E.4: Required automated mechanisms like Data Loss Prevention (DLP) scanning to verify PII inventory accuracy and reconcile data flows. • Section III.E.5: Added reference to the Security Metrics Standard for defining and reporting performance metrics monthly. • Section III.E.6: Mandated security reviews during the architectural design phase for all new projects. • Section III.E.7: Required documentation of resilience strategies in the Critical Infrastructure and Key Resources Protection Plan. • Section III.E.11: Established a Cross-Discipline Insider Threat Team with a required quarterly meeting cadence. • Section III.F: Added a definition for Plan of Action and Milestones (POA&M).	DCH CISO