GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**549**	**Division:**	**Office of Information Technology**
Policy Title:	**Supply Chain Risk Management (SR)**	**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, the development, implementation and administration of an overall Supply Chain Risk Management (SR) 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 comply with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Supply Chain Risk Management (SR) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Systems and Supply Chain Risk Management (SR) 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 Supply Chain Risk Management (SR) 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 Supply Chain Risk 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 Supply Chain Risk Management policy and procedure in addition to managing the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Supply Chain Risk Management policy and plan that addresses purpose, scope, roles, and procedures. Procedures shall include implementation of the Supply Chain Risk Management policy and the associated Risk Assessment controls.
2. Develop, document, and implement a separate plan to manage supply chain risks for all DCH information systems, services, and components containing sensitive and confidential information.
    - Review and update the plan on an annual basis or as dictated by evolving risks/threats and changes to the environment.
    - Protect the plan from unauthorized access, modification, and disclosure.
    - Establish a DCH-wide Supply Chain Risk Management (SCRM) team to oversee and manage the program by assessing, identifying, managing, and mitigating supply chain risks.
3. Document and establish a process to identify, remediate, and prevent deficiencies and vulnerabilities in the supply chain process.
    - Document and deploy controls to protect against risk to the supply chain system and process and limit the impact of such events.
    - Document the selected and implemented supply chain processes and controls in the applicable SSP or a dedicated supply chain risk management plan.
    - Diversify the supply chain systems and components to reduce an adversary's risk of successfully disrupting or shutting down the supply chain.
    - Ensure that all controls stated in vendor contracts are also stated and agreed upon by sub-contractor agreements.
4. Ensure that the Provenance (see definition) of all systems, components, and data are documented, tracked, accounted for, and maintained from the point of origin to changes and updates.
    - Establish, document, and maintain visibility into supply chain activities, processes, and personnel.
    - Establish unique identifiers for tracking supply chain elements, systems, and components.
    - Identify and deploy controls to ensure that received systems and components are authentic and have not been tampered with.
    - Employ the controls to ensure system and component integrity by validating asset Provenance and composition of components for critical assets.

5. Develop and implement an acquisition process that accounts for protective measures and due diligence for mitigating supply chain risks when procuring systems, products, and services.
    - Ensure an adequate supply of systems and components are in place by continuously monitoring performance, availability, and capacity plus ensuring multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission-critical times, and identifying substitute components to be deployed.
    - Perform system component assessments before acquisition selection, acceptance, upgrades, and updates.
6. Perform supply chain risk assessments with suppliers and contractors of their services and systems.
7. Establish agreements and procedures that state notification requirements and responsibilities for all parties involved in the supply chain process.
8. Perform physical inspections on systems and components to periodically detect physical and logical tampering.
    - Inspections can include detection of packaging changes, tamper-resistant broken seals, counterfeit parts substitutions, skimmers, etc.
9. Develop, document, implement, and maintain an anti-counterfeiting program, including detecting counterfeit (and substandard) components from entering or being inserted into systems.
    - Maintain full configuration control over systems and components awaiting or undergoing repairs, maintenance, and upgrades before returning to service and connecting to DCH networks and resources.
10. Dispose of data, documentation, tools, or system components using DCH approved methods (to prevent opportunities for compromise) in alignment with the Media Protection policy and procedure.

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.
- 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.
- Provenance – The tracking of the origin, development, ownership, location, and changes to a system or system component and associated data.
- SCRM – Supply Chain Risk Management - Systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk responses.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.
- Supply Chain - Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, which begins with the sourcing of products and services and extends through their life cycle.
- Supply Chain Element - Organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components.
- SSP - System Security Plan that documents how an organization implements its security requirements and security guidelines and standards that the organization follows.
- Vulnerability - A security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered.

F. Please refer to NIST 800-53 Supply Chain Risk Management (SR) Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Supply Chain Risk Management.

November 23, 2023

Signature ***Date***