GEORGIA DEPARTMENT OF COMMUNITY HEALTH		**Enterprise Policy**	
Policy No.:	545	**Division:**	**Office of Information Technology**
Policy Title:	Risk Assessment (RA)	**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 Risk Assessment (RA) 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 Risk Assessment (RA) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Risk Assessment (RA) 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 Risk Assessment (RA) 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 policy is to implement and manage a formal Risk Assessment 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 Risk Assessment policy and procedure and manage the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Risk Assessment policy and plan that addresses purpose, scope, roles, and procedures. Procedures shall include implementing the Risk Assessment policy and the associated Risk Assessment controls.

2. Categorize each system and the information being processed, transmitted, and stored.
   - Include the categorization and the rationale in each System Security Plan (SSP) in alignment with NIST-FIPS 199 for the categorization of risk.
   - Obtain approval from the authorizing individual (Business Owner) for each security categorization.
   - Identify and document impact levels for each system (what is the impact to the organization if this system is not operational?)

3. Conduct a Risk Assessment that covers the following:
   - Identifies all threats and vulnerabilities to systems that process, store, and/or transmit sensitive information.
   - Determine the likelihood and impact of adverse events occurring while processing sensitive information.
   - Incorporate the results of risk assessments and business risk management decisions into the system risk assessments.
   - Document and review the risk assessment results.
   - Update risk assessment (and supply chain risk assessment) upon environmental and regulatory changes or introduction of new threats/vulnerabilities. Continuously monitor the cyber threat landscape and adjust as needed.
   - Assess supply chain risks associated with defined critical systems and vendors.
   - Utilize All-Source Intelligence to analyze risk.
   - Implement automation and analytics techniques to predict and prepare for risks.

4. Implement a vulnerability identification, response, and management program that:
   - Scans for vulnerabilities in identified systems and applications.
   - Deploys tools to identify vulnerabilities (e.g., software flaws and configuration issues).
   - Analyze and gauge the impacts of identified vulnerabilities.
   - Eradicate vulnerabilities in alignment with Risk Assessment processes.
   - Share and disseminate vulnerability reports for awareness and remediation planning purposes.
   - Update vulnerability scanning tools to look for new vulnerabilities when they are identified and reported before the next scan occurs.
   - Identify in-scope systems for vulnerability assessments (e.g., all systems containing sensitive and confidential information).
   - Document corrective actions to be taken and the process for performing remediation.

- o Ensure that vulnerability scanning activity aligns with privileged user management.
- o Identify trends by comparing historical and current scans to determine direction better and identify patterns.
- o Review historic logs regarding previously exploited vulnerabilities for forensic and future awareness and response to similar exploits.
- o Correlate vulnerability scanning output to identify multiple attack paths taking place simultaneously.
- o Implement a publicly discoverable reporting channel that discloses newly discovered vulnerabilities.
5. Implement and deploy a counter surveillance program to detect the presence of technical surveillance devices and identify technical security weaknesses.
6. Respond to findings reported by all Security, Risk, and Privacy assessments, monitoring, and audits.
7. For systems (or software) that process sensitive information, conduct a privacy impact analysis before procuring or developing the products and:
    - o Identifying the new sensitive information that will be processed, including the PII permitting the contacting of individuals.
8. Perform Criticality Analysis to identify critical systems, components, and processes.
9. Develop and implement a Cyber Threat Hunting program to include:
    - o Detect and resolve instances of system compromises and threats that have evaded existing controls.
    - o Perform threat hunting annually.

E. Definitions

- All-Source Intelligence – Products and/or organizations and activities that incorporate all sources of information.
- 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.
- 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.
- 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. References: Please refer to NIST 800-53 Risk Assessment (RA) Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Risk Assessments.

_____   11/12/2023
_____

Signature   *Date*