GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**537**	**Division:**	**Office of Information Technology**
Policy Title:	**Incident Response (IR)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

In order 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 Incident Response (IR) 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 Incident Response (IR) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Incident Response (IR) 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 Incident Response (IR) 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 having connectivity to the network are 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 Incident Response 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 Incident Response 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 Incident Response Policy and plan that addresses the purpose, scope, roles, and procedures to implement incident response protocols. The NIST standard is adhered to for Cyber Security Incidents, and the HIPAA Incident Response Policy and Procedure document is followed for Privacy Incidents.
2. Provide incident response training to personnel assuming an incident response role during orientation and/or upon system changes or as the follow-up to an incident.
    - Provide general training to all personnel (e.g., how to identify and report an incident, information to capture, etc.) as part of security awareness training during new hire orientation.
    - Simulate actual events (e.g., TableTop scenario) into incident response training (incorporate automated mechanisms such as alerts).
    - Include training on identifying and reporting of data breaches.
3. Test the effectiveness of the incident response program (e.g., via exercises, Tabletops, etc.) to determine the efficacy and opportunities for improvement.
    - Incorporate automation into incident response testing (e.g., alerts).
    - Coordinate incident response testing with multiple areas, including Disaster Recovery and Business Continuity personnel in addition to Business Unit representatives. (Note: there are currently touchpoints between the groups incorporated into processes.)
    - Develop and plan to address identified quantitative and qualitative gaps.
    - Utilize metrics to measure against agreed upon service levels, standards, and baselines.
4. Develop and implement a standardized comprehensive incident handling plan across the organization.
    - Incorporate preparation, prevention, detection, analysis, containment, eradication, and recovery into the plan.
    - Integrate incident response plan into overall contingency plan (business continuity and disaster recovery).
    - Incorporate lessons learned and root cause analysis into the incident response plan.
    - Utilize automated incident management tools when feasible.
    - Define and document classes of incident criticalities (e.g., critical, high, medium, low) to prioritize response during incidents.
    - Enhance organizational awareness by correlating incident information from different sources and coordinating information sharing with external organizations when applicable (e.g., supply chain events with suppliers, customers, and service providers).

- Identify thresholds or events requiring turning off a system should the event occur (tie into the Disaster Recovery Plan). Implement a solution that would disable the impacted system.
- Incorporate a documented protocol for handling insider threats. Background checks are performed on prospective employees and contractors who have access to sensitive information.
- Establish an Incident Response team that is available 24/7 and can be quickly deployed.
- Following an incident, perform analysis on malicious code in an isolated or dedicated environment to help prevent and prepare for future incidents. Impacted machines are immediately isolated, and digital forensics are generated as appropriate.
- Perform anomalous behavioral analysis to understand adversarial tactics better and identify potential red flags.
- Ensure that someone is tasked with managing external corporate communications and public relations and can mitigate any reputational concerns following an incident.

5. Track and document incidents from identification until closure.
    - Use a tool to enter and track all incident related information.
6. Require personnel to report suspected incidents to the Information Security Office mailbox (DCHOIS@DCH.GA.GOV).
    - Document process for reporting incidents to external parties (e.g., law enforcement, Cyber insurance providers, customers, regulators, vendors, etc.)
    - Report identified system vulnerabilities to the Cyber Security Office.
    - Develop a process related incidents to external supply chain parties (e.g., service providers, vendors, distributors, manufacturers, etc.)
7. Provide incident response assistance via organizations such as a Help Desk, Incident Response Team, Emergency Response Team, etc., and tools for managing and tracking incidents.
    - Document and record all external service providers' functions and contact information.
8. Develop and document an incident response plan that, at a minimum, shall include:
    - The organizational mission and roadmap for implementation.
    - Structure, resources needed, and organization for effectively managing the Incident Response function.
    - Coordination with other areas (e.g., Business Continuity Disaster Recovery function)
    - Communications and distribution plan and protection from unauthorized disclosure and modification.
    - Provide metrics for measuring effectiveness and capacity (e.g., SLAs, response time, open tickets over time, etc.)
    - Designates CISO responsible for Incident Response (e.g., Incident Response Coordinator, Help Desk Manager, etc.)
    - Document within the plan the means, extent, and circumstances for communication of incidents.

- Develop a plan to identify privacy concerns and subsequent actions and mitigation of any adverse impacts to individuals or groups.

9. Respond and recover from Information Spillage by implementing the following measures:
    - Designation of a responsible function or individual who is responsible for responding, communicating, and mitigating the event.
    - Process to identify impacted information/systems and perform isolation and eradication measures.
    - Provide training on identification and responding to Information Spillage as well as applicable laws, policies, and directives.
    - Develop a workaround plan for continued operations during an Information Spillage event impacting systems.

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.
- Information Spillage - Release or loss of sensitive information to unauthorized recipients (persons, systems, applications, or media).
- 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:
        i. Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
        ii. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
        iii. Employment records held by DCH (a covered entity) in its role as employer; and

iv. 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.
- SLA – Service Level Agreement to establish and measure an agreed upon level of performance or standard.

F. References: Please refer to NIST 800-53 Incident Response (IR) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Contingency Planning.

11/12/2023

Signature ***Date***