GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**535**	**Division:**	**Office of Information Technology**
Policy Title:	**Contingency Planning (CP)**	**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 Contingency Planning (CP) 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 Contingency Planning (CP) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Contingency Planning (CP) 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 Contingency Planning (CP) 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 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. It is the policy of DCH to implement and manage a formal Contingency Planning (CP) program.

B. DCH shall implement and disseminate this Contingency Planning (CP) policy and procedures to all personnel and contractors.

C. The Chief Information Security Officer is designated to manage the development, documentation, implementation, and dissemination of the Contingency 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 Disaster Recovery Plan (DRP) that addresses recovering one or more information systems in response to a major hardware or software failure or destruction of facilities. The documented plan shall address the following areas:
    - Identifies critical business functions and systems by performing a Business Impact Analysis ("BIA") with DCH business units.
    - From the Business Impact Analysis, identify Recovery Time Objectives and Recovery Point Objectives for each critical system or process.
    - Identifies all relevant roles and responsibilities in addition to current contact information.
    - Identifies and documents temporary workarounds when a disruptive event takes place.
    - Documents the steps needed for recovery and restoration without degrading security controls.
    - Incorporate lessons learned from testing or training exercises and actual contingency events. Update plans based on gaps identified during the lessons learned phase.
    - Include the steps needed to declare an end to the event and resumption of normal business activities.
    - Identify all alternate processing and storage sites to be deployed in the event of a contingency event.
    - Identify all Service Providers (e.g., vendors, utilities, insurance providers) and record contact information.
2. Coordinate contingency planning with incident planning and response.
3. Review and update the contingency plan at least annually or as dictated by contingency events and/or organizational, environmental, or regulatory changes.
4. Incorporate capacity planning into contingency planning.
   Provide Contingency Training to all system users and those responsible for performing contingency roles at least annually or as determined by system changes or lessons learned following an event. Training shall be reviewed and updated based on lessons learned from actual events or as environmental changes require. Training shall incorporate simulation of actual events to gauge personnel response to life-like situations.
5. Test the contingency plan on a frequency DCH determines based on priorities determined by Recovery Time and Recovery Point Objectives and Business Impact Analysis.
    - Testing shall be performed by individuals tasked with response and recovery roles as well as Business Unit testers evaluating functionality for their systems and applications. Testing shall also include a simulation of a disruptive system event to assess the plan's effectiveness.

    - Perform testing at an alternate processing (or testing) site.
    - Include full recovery and restoration as part of the testing strategy.
6. Establish an alternate dedicated processing and storage site for deployment during an actual contingency event. The site can be physical or logical and geographically separated from the primary site to reduce the impact of a widespread disaster event. Enable the alternate site to support Recovery Time and Recovery Point objectives.
7. Ensure adequate equipment and supplies are available at the alternate site to support response, recovery, and restoration activities while subject to the same controls at the primary site. Plan for the site to be fully operational during a contingency event that may preclude returning to the primary site for a period of time.
8. Ensure that alternate or backup telecommunications services are in place during a contingency event to avoid a single point of failure. As part of this process, DCH will:
    - Determine that service agreements account for the need to deploy alternative telecommunications services when required.
    - Validate as part of Service Provider management that the vendors have their own contingency plans in place, have tested such plans, and can provide evidence of testing.
    - Ensure that alternate communication services are addressed in the Contingency Plan and as part of testing protocols.
9. Shall perform restorable data backups of user level and system level/documentation in a secure manner at a frequency based on system criticality, Recovery Time, and Recovery Point Objectives.
10. Shall ensure that backups are stored in a redundant secondary repository.
11. The backup process shall be tested to ensure the adequacy of the backups (reliability and integrity), and that backed-up data can be effectively restored to the desired recovery point objective. This process will:
    - Incorporate sample backup restoration into contingency testing protocols.
    - Ensure dual authorization is implemented for the destruction of backup data.
    - Deploy cryptographic mechanisms to protect backed-up data in storage against unauthorized disclosure or modification.
12. Reconstitute and recover systems to the last known operational state within the stated Recovery Time Objectives (including transaction recovery).
13. Deploy alternative security mechanisms when the primary security mechanisms are unavailable or compromised (e.g., different methods of authentication when one mode of authentication is unavailable.)

E. Definitions

- Business Impact Analysis – A process to identify all critical systems and processes that will then determine recovery prioritization during a disaster or business continuity event.
- Contingency Planning (CP) – The development and implementation of a program to prepare for, respond, mitigate, and recover from impactful Disaster Recovery and Business Continuity events.

- Disaster Recovery Plan (DRP) - A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
- 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.
- 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.
- Recovery Time Objective - How soon you need to restore your system before an outage incurs a large, potentially business threatening impact on your entity.
- Recovery Point Objective - The point in your backups you want to restore your system from (e.g., 24 hours ago).
- Recovery Time Actual - How long does it take to recover your system during a Disaster

- Recovery test or event. The RTO will be compared to the RTO for assessing the effectiveness of the recovery.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.

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

November 29, 2023

Signature ***Date***