GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**534**	**Division:**	**Office of Information Technology**
Policy Title:	**Configuration Management (CM)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

To identify unauthorized access to the Agency's sensitive information. The purpose of this document is to establish procedures for the implementation of the Configuration Management (CM) program that are authorized to operate within the sensitive information environment;

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 Configuration Management Control (CM) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Configuration Management (CM) 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 Configuration Management (CM) 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 Configuration Management program.

B. DCH shall implement and disseminate Configuration Management policies 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 the Configuration Management policy and procedures in addition to the program.

D. In accordance with this policy, DCH shall:

1. Develop a minimum system security baseline configuration.
    - Review and update the baseline at least annually (or as required) or when system components are introduced or upgraded.
    - Retain previous versions of the system security baseline to support rollback or failover efforts and for historical reference.
    - Maintain a separate baseline for test and development environments.
    - Implement additional controls (e.g., limited applications, sanitized hard drives, etc.) on devices (e.g., laptops, mobile phones) when individuals travel to high-risk locations and restore the devices to the previous version upon return.
2. Define configuration changes that fall under the requirements of the Change Management policy.
    - Include Information Security representation for Change Management to review upcoming changes to ensure that the proposed change aligns with DCH baselines and requirements.
    - Identify and review the security and impact of configuration changes before being allowed to implement the change.
    - Document the proposed change and a back-out or rollback plan.
    - Perform changes in alignment with the current baseline and requirements.
    - Document a plan for testing and validating the change. Perform validation testing prior to change implementation and following change implementation.
    - Document all configuration modification change decisions (approvals, rejections, requests for more information).
    - Issue alerts when unauthorized configuration changes are detected for subsequent remediation.
    - Retain records of configuration changes for a period at least annually (or as required).
    - Monitor and review the configuration changes.
    - Manage cryptographic mechanisms (e.g., certificates, keys) within configuration management.
    - Review changes to detect unauthorized changes.
    - Restrict system configuration changes (outside of emergency changes) to designated change windows or to a time when the change is least disruptive to operations.
3. Perform analysis to determine the impact of proposed changes to privacy and security. Impact analysis will be performed prior to change approval and implementation.
    - Analyze change impact in a separate and/or dedicated test or development environment.

    - After the change, validate that the implemented updates have been performed correctly and are working as intended with no degradation to security and privacy requirements.
4. Implement and enforce logical and physical access restrictions to the system associated with the change.
    - Generate audit trails to capture any updates.
    - Enforce dual authorization for approving and implementing changes.
    - Limit privileges to perform system configuration changes in a production environment and review those privileges on a periodic basis.
5. Determine, document, and implement all configuration settings (baselines, parameters).
    - Utilize automated tools to manage, apply, and validate configuration settings.
    - Perform required actions when unauthorized configuration changes are detected.
6. Configure systems to support Least Functionality (e.g., least privilege, minimum necessary).
    - Review systems to identify, track, and subsequently remove/disable unnecessary and/or nonsecure functions, ports, protocols, software, and services.
    - Prevent execution of programs in alignment with DCH policies and standards.
    - Protect systems with deny-all by default and permit by exception policy.
    - Identify user-defined software that is required to be installed in a dedicated environment due to potential malware concerns or unknown origin.
    - Disallow the use of unauthorized hardware components and binary executable code from untrusted sources (e.g., public and unvetted software).
7. Develop, document, and maintain a system component inventory in a centralized repository, which is reviewed and updated at least on an annual basis or when there are changes to inventory components (e.g., installations, removals, and updates).
    - Detect the presence of unauthorized system components (hardware, software, etc.)
    - Document who is responsible or contact personnel for inventoried system components and assign each component to a specific system.
    - Note deviations or exceptions from approved configuration settings or minimum security baselines.
    - Deploy automated mechanisms to maintain and track system components geographically.
8. Establish, document, and maintain an approved configuration management plan that addresses roles and responsibilities, identifies and places components under the configuration management purview, and is protected from unauthorized modification and disclosure.
    - Maintain separation of duties between the role that maintains the plan and those involved in system development.
9. Control and track software proliferation and usage in accordance with contractual requirements, licensing agreements, and copyright laws.
    - Restrict the use of Open Source Software

    - Monitor for the unauthorized use, distribution, and reproduction of copyrighted software.
10. Determine and enforce who can install software and limit the privileges.
11. Enforce software installations via monitoring to identify any unauthorized software installs.
12. Identify and document all users with access to DCH information systems and an inventory of the systems where the information resides.
    - Deploy the use of automated tools where feasible to detect and manage user and information listings and to enforce existing controls.
13. Develop a documented plan for mapping data actions (processing, sharing, disclosing, retention, and disposal).
14. Require digital signatures and organization-approved certificates to validate the installation of software and firmware.

E. Definitions

- Binary Executable Code – A program that performs a set of instructions on an operating system.
- Data Mapping – Matching data fields from one database to another.
- 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.
- Least Functionality (Minimum Necessary) – Granting the minimum access needed to perform a specific job role or function.
- NIST – The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See https://www.nist.gov/.
- Open Source Software – Copyright holder grants users the rights to change and distribute the software to anyone with no restrictions.
- 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.
- Role Based Access – Access Group or profile based on defined job functionality within a department or team.
- Sensitive Information - PII, PHI, ePHI, proprietary/trade secret and similar data that require special handling.

F. References: Please refer to NIST 800-53 Configuration Management (CM) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Configuration.

November 29, 2023

Signature ***Date***