GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**538**	**Division:**	**Office of Information Technology**
Policy Title:	**Maintenance (MA)**	**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 Maintenance (MA) 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 Maintenance (MA) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Systems and Maintenance (MA) 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 Maintenance (MA) 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 maintenance 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 the Maintenance policy and procedures and manage the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Maintenance Policy and plan that addresses purpose, scope, roles, and procedures.
2. Formally establish a maintenance management program that would establish controls for:
    - Schedule, document, and review records of maintenance, repair, and replacement of system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
    - Approve (in writing) all on-site or remote maintenance activity (and note the distinction), including removing equipment from the physical site for maintenance, repair, replacement, or disposal.
    - Sanitize all equipment before it is removed from the physical facility or disposed of. The Agency and vendors shall follow the Media Sanitization Standards of the most current version of NIST 800-88.
    - Verify that pre-existing security controls are still in place following maintenance and/or repair (e.g., run against security baseline).
    - Require that formal maintenance records are created, maintained, contain information, and are retained for at least seven years minimum as required by the Georgia Secretary of State Data Retention schedule.
    - Restrict the use of maintenance tools to authorized personnel only.
3. Identify, document, manage, and monitor the use of system maintenance tools (e.g., hardware and software).
    - Perform period inspections of maintenance tools to detect unauthorized updates and ensure the latest software updates and patches are installed**.**
    - Monitor the use of maintenance tools that run with elevated privileges.
    - Perform checks on media (being used for diagnostic or maintenance purposes) for malicious code before deploying the media.
4. Before equipment is removed, verify the following:
    - All organizational information within the equipment has been removed and/or the equipment has been sanitized or destroyed.
    - Obtain a documented exception if the above cannot be met.
5. Employ the following controls when non-local maintenance is being performed:
    - Approve, allow, and monitor non-local maintenance in accordance with DCH policies and procedures.
    - Ensure strong authentication protocols are in place before allowing non-local maintenance and terminate network connections when the activity has been completed.
    - Maintain non-local maintenance records for a period of at least seven years.
    - Review audited records of non-local maintenance to detect anomalies or unauthorized activities.

- Ensure that non-local maintenance is performed from a system whose security controls are comparable to or equal to DCH's.
- Ensure that the component to be removed is sanitized prior to maintenance and then inspected and tested for malware before reinstallation or connection.
- Separate the maintenance activity logically or physically from other network sessions.
- Ensure that notice is provided as to the time and date of maintenance and that each maintenance session has been approved.
- Deploy cryptographic mechanisms for non-local maintenance activities.
- Validate that session and network sessions have been terminated following completion of maintenance. (Note: In some cases, the access may be disabled following the maintenance)

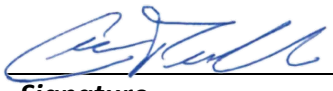
6. Maintain a list of all maintenance organizations with names, contact information and purpose.
    - Ensure that maintenance personnel are escorted while on the premises or have the required authorization not to be escorted.
    - Deploy knowledgeable personnel to supervise maintenance activities for those without the required access authorizations.
    - Implement procedures to manage and monitor those maintenance personnel who do not possess the appropriate access authorizations (e.g., Federal Secret Clearance).
    - Develop and document workarounds or compensating controls to protect modules that cannot be sanitized or removed from the system for maintenance.
7. Perform maintenance in a timely manner and employ preventative maintenance in alignment with manufacturer specifications.
8. Perform maintenance to monitor equipment health and performance.
9. Utilize a maintenance management system for planning, scheduling, record keeping, and reporting.
10. When possible, restrict field maintenance on critical or sensitive systems to on-site only.

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/.
- Non-Local Maintenance - Servicing equipment remotely.
- 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.

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



November 23, 2023

Signature ***Date***