 <b>GEORGIA DEPARTMENT OF COMMUNITY HEALTH</b>		<b>Enterprise Policy</b>	
<b>Policy No.:</b>	<b>538</b>	<b>Division:</b>	<b>Office of Information Technology</b>
<b>Policy Title:</b>	<b>Maintenance (MA)</b>	<b>Effective Date:</b>	<b>December 17, 2025</b>
<b>Version:</b>	<b>3</b>	<b>Category:</b>	<b>Cybersecurity Governance, Risk, and Compliance</b>

### 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 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 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. This plan shall include specific Standard Operating Procedures (SOPs) for all critical maintenance activities (e.g., patching, sanitization) and define the frequency and roles responsible for execution.
  - 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. Approvals must be granted by the System Owner or designated Information System Security Officer (ISSO) prior to work commencement.
    - Sanitize all equipment before it is removed from the physical facility or disposed of in accordance with DCH Enterprise Policy - Media Protection (No. 539) and NIST SP 800-88. 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 sufficient detail to support audit and accountability activities, and are retained for a period consistent with applicable legal, regulatory, and records-management requirements, including the Georgia Secretary of State Records Retention Schedules.
    - 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). A register of approved maintenance tools shall be maintained by the Security Operations team and reviewed annually for continued business need and security compliance.
  - 4. Perform period inspections of maintenance tools to detect unauthorized updates and ensure the latest software updates and patches are installed.
  - 5. Monitor the use of maintenance tools that run with elevated privileges via automated logging and periodic audit review to detect unauthorized access or modification.
  - 6. Perform checks on media (being used for diagnostic or maintenance purposes) for malicious code before deploying the media. All diagnostic media and maintenance

- tools must be scanned for malicious code using organization-approved antivirus solutions prior to connection to any DCH system.
7. Before equipment is removed, verify the following:
  8. All organizational information within the equipment has been removed and/or the equipment has been sanitized or destroyed.
  9. Obtain a documented exception if the above cannot be met.
  10. The Maintenance policy and procedures shall be reviewed annually to ensure their continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy and/or procedures shall be updated to reflect changes in relevant factors, such as assessment or audit findings; security or privacy incidents; and changes to applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. The revised policy and/or procedures shall be communicated to all affected parties.
  11. The DCH System Security Plan (SSP) must be updated as part of the annual review process, or whenever significant changes occur that could impact system security, including new vulnerabilities, operational changes, or legal and regulatory requirements. All updates to the SSP must be documented and approved by the CISO or designated authority. The updated SSP shall be distributed to relevant stakeholders to ensure awareness and compliance.
  12. Employ the following controls when non-local maintenance is being performed:
  13. Approve, allow, and monitor non-local maintenance in accordance with DCH policies and procedures.
  14. Ensure strong authentication protocols are in place (Multi-Factor Authentication compliant with NIST SP 800-63B) before allowing non-local maintenance and terminate network connections when the activity has been completed.
  15. Maintain non-local maintenance records for a period of at least seven years.
  16. Review audited records of non-local maintenance to detect anomalies or unauthorized activities. Logged events must include session start/end times, user identity, and all privileged commands executed during the session.
  17. Ensure that non-local maintenance is performed from a system whose security controls are comparable to or equal to DCH's.
  18. Ensure that the component to be removed is sanitized prior to maintenance and then inspected and tested for malware before reinstallation or connection.
  19. Separate the maintenance activity logically or physically from other network sessions.
  20. Ensure that notice is provided as to the time and date of maintenance and that each maintenance session has been approved.
  21. Deploy cryptographic mechanisms for non-local maintenance activities.
  22. 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)
  23. Maintain a centralized, up-to-date list of all maintenance organizations with names, contact information, and purpose. Access authorizations for these personnel shall be verified against this list prior to granting facility or system access.
  24. Ensure that maintenance personnel are escorted while on the premises or have the required authorization not to be escorted.


25. Deploy knowledgeable personnel to supervise maintenance activities for those without the required access authorizations.
26. Implement procedures to manage and monitor those maintenance personnel who do not possess the appropriate access authorizations (e.g., Federal Secret Clearance).
27. Develop and document workarounds or compensating controls to protect modules that cannot be sanitized or removed from the system for maintenance.
28. Perform maintenance in a timely manner and employ preventative maintenance in alignment with manufacturer specifications. Maintenance response times and repair SLAs must align with the Recovery Time Objectives (RTOs) defined in the system's Business Continuity and Contingency Plan (Policy No. 535).
29. Perform maintenance to monitor equipment health and performance.
30. Utilize a maintenance management system for planning, scheduling, record keeping, and reporting.
31. 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.



*Signature*

12/18/2025  
*Date*

**Revision History**

Version	Date	Description	Author
1.0	11/23/2023	Reviewed and approved by DCH CIO; establishing v1.0	DCH CISO
2.0	11/08/2024	<ul style="list-style-type: none"> <li>• Added a revision history table to validate consistent review/update and document changes</li> <li>• Section D.5: The Maintenance Policy shall be reviewed annually</li> <li>• Section D.6: The SSP shall be reviewed annually</li> </ul>	DCH CISO
3.0	12/17/2025	<ul style="list-style-type: none"> <li>• Section III.D.1: Updated to mandate specific Standard Operating Procedures (SOPs) for critical maintenance activities, defining frequency and execution roles.</li> <li>• Section III.D.2: Amended bullets 2 and 3 to require explicit approval from System Owners or ISSOs prior to maintenance and mandates sanitization in accordance with DCH Policy 539 and NIST SP 800-88.</li> <li>• Section III.D.3: Updated to require a register of approved maintenance tools maintained by Security Operations and reviewed annually.</li> <li>• Section III.D.5: Updated to mandate automated logging and periodic audit review for maintenance tools running with elevated privileges.</li> <li>• Section III.D.6: Added requirement to scan all diagnostic media and maintenance tools for malicious code using approved antivirus solutions prior to connection.</li> <li>• Section III.D.10 Added specific definitions for organization-defined events, including assessment findings, incidents, and legal/regulatory changes, and updated terminology to explicitly reference "policy and procedures" to clarify the full scope of requirements.</li> </ul>	

		<ul style="list-style-type: none"><li>• Section III.D.14: Updated to mandate Multi-Factor Authentication compliant with NIST SP 800-63B for non-local maintenance sessions.</li><li>• Section III.D.16: Expanded logging requirements for non-local maintenance to include session start/end times, user identity, and privileged commands.</li><li>• Section III.D.23: Updated to require a centralized, up-to-date list of maintenance organizations for verifying access authorizations.</li><li>• Section III.D.28: Aligned maintenance response times and repair SLAs with Recovery Time Objectives (RTOs) defined in the Business Continuity and Contingency Plan (Policy No. 535).</li></ul>	
--	--	---	--