GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**548**	**Division:**	**Office of Information Technology**
Policy Title:	**Systems and Information Integrity (SI)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

To adequately protect sensitive information from losses due to the accidental or intentional misuse of information technology resources, the development, implementation, and administration of an overall Systems and Information Integrity program is critical. The term "sensitive" refers to PII, PHI, ePHI, SSA PII, and similar data that require special handling. This document guides the creation and maintenance of 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 Systems and Information Integrity (SI) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Systems and Information Integrity (SI) 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 Systems and Information Integrity (SI) 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 Systems and Information Integrity 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 ("CISO") to manage the development, documentation, implementation, and dissemination of this Systems and Information Integrity policy and procedure and manage the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Systems and Information Integrity policy and plan that addresses purpose, scope, roles, and procedures.
2. Implement a process for flaw remediation to include:
    - Testing software and firmware updates in coordination with flaw remediation to determine potential security impacts before installation.
    - Install required software patches or implement a Plan of Action and Milestones ("POAM") within 30 days of the release for critical patches.
    - Align flaw remediation into the Configuration management program and maintain security baselines.
    - Determine if planned upgrades, patches, etc., have applicable security components.
    - Document the time between flaw identification and remediation and establish baselines for corrective actions.
    - Deploy automated tools to support patch management implementations.
    - Remove previous versions of software once updates have been installed and validated.
3. Implement malicious code measures to detect and eradicate malware at system entry and exit points in alignment with the Incident Response plan.
    - Update malicious code signatures and methodologies as new releases are available in alignment with DCH configuration management requirements.
    - Perform periodic scans of the system and files from external sources that are downloaded, stored, opened, and executed.
    - When identified, block and quarantine malicious code and provide communication alert via ticket opened by the Help Desk and communicated to the Office of Information Security and state service providers**.**
    - Implement a process to account for and test for identifying false positives (e.g., benign code identified as malware) and the system impact.
    - Update malicious code protection mechanisms and signatures only at the direction of an authorized privileged user.
    - Detect malicious commands within the criteria of command types, command classes, or specific instances of command. Determine how these commands will be handled (e.g., warning before the command is executed, prevention or audit of command executed.)

- Deploy tools to analyze malicious code and align the results into the Incident Response Plan and flaw remediation activities.

4. Perform system monitoring to detect and alert on the following activities:
    - Attacks and indicators of potential attacks.
    - All unauthorized connections (e.g., local, network, and remote).
    - Unauthorized system use.
5. Deploy monitoring devices and capabilities within critical systems and track critical transactions.
    - Perform analysis on identified anomalies and perform follow-up actions.
    - Adjust monitoring to reflect changes in risk, requirements, environment, operations, and individuals.
    - Deploy an enterprise-wide Intrusion Prevention/Intrusion Detection system.
    - Implement an automated Security Information and Event Management ("SIEM") for capturing, alerting, and analyzing real-time events.
    - Integrate Intrusion Prevention/Intrusion Detection tools with access and flow control to help isolate attacks.
    - Monitor for unauthorized or unusual inbound and outbound communications to detect covert data exfiltration and analyze anomalies.
    - Collect info and notify the Information Security Office when compromises, intrusions, unusual activities with security and privacy implications, and potential compromises occur, align with the Incident Response plan, and take appropriate actions.
    - Perform testing on Intrusion Prevention/Intrusion Detection systems.
    - Determine the balance between communications encryption and the visibility of information.
    - Monitored and audited information shall be correlated for a more complete view and identification of activity patterns. In addition, correlate information from physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.
    - Implement monitoring and logging of privileged user activities.
    - Implement a process to detect unapproved and unauthorized network services and alert the Information Security Office when such anomalies are identified.
    - Monitor and analyze network traffic at external and key internal system interfaces to maximize monitoring effectiveness.
6. Implement a process to receive security alerts and advisories.
    - Disseminate general internal security alerts and directives to DCH personnel as appropriate.
    - Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.
    - Broadcast security alerts and advisory information throughout the organization using appropriate methods such as email and Intranet Portal.
7. Implement a process and tool (e.g., cryptographic) for performing integrity checks to detect unauthorized changes to software and data and subsequent actions to take when anomalies are identified.
    - Ensure that integrity checks using centrally managed tools are performed during transitional states such as start-up, shutdown, new hardware installations, etc.

- Deploy automated tools to notify when integrity anomalies are discovered.
- Perform automatic system shutdowns and re-starts when integrity anomalies are identified.
- Incorporate detection and follow-up actions on unauthorized changes into the Incident Response Plan.
- Ensure the capability to audit the event related to integrity issues (unauthorized changes) and perform the follow-up action when identified.
- Perform cryptographic authentication checks on software before installation and integrity checks on user-installed software before installation and execution to prevent the introduction of malicious code or programs.
- Apply time limits on running and executing processes without supervision.
- Implement runtime application self-protection technology to detect and prevent the exploitation of vulnerabilities while software is executing.

8. Deploy spam protection at entrance and exit points to detect and act on identified spam.
    - Employ automated mechanisms to update spam protection methodologies and provide a learning capability to identify legitimate emails and avoid acting upon false positives.
9. Ensure that error handling processes are in place to generate error messages with sufficient information to act upon and perform corrective actions without revealing exploitable information.
    - Error messages shall be restricted to authorized personnel.
10. Implement an information management retention program in compliance with applicable laws, executive orders, directives, regulations, and DCH records retention requirements and schedules.
    - Restrict, mask, or limit the use of Sensitive Information throughout the information lifecycle.
    - Utilize techniques such as de-identification, masking, scrambling, or synthetic data to minimize the use of sensitive information for testing, training, and research (analysis).
    - Use DCH approved methods for disposing, destroying, and erasing information following the end of the retention period when it is no longer needed.
11. Determine MITF (Mean Time To Failure) on system components and, as a preventative measure, provide compatible replacement components following manufacturers' criteria.
    - Transfer system component's responsibility to substitute components within the appropriate time to reduce the risk of degraded or interrupted business functions.
    - Initiate manual transfers between active and stand-by components upon reaching the appropriate percentage of MITF.
    - Upon detecting system component failures, ensure that the stand-by components are successfully installed and operational and prepare to manually or automatically shut down the system.
    - Provide automatic failure capability to an alternate system upon the failure of the primary system.
12. Implement Non-Persistence to reduce the targeting capability of adversaries (i.e., the window of opportunity and available attack surface) to initiate and complete attacks.

- Ensure that software and data used for refreshes are from trusted sources.
- Retain information no longer than needed or required and delete in alignment with DCH requirements.
- Establish system connections on-demand when needed and terminate connections when no longer needed.

13. Verify output results from software programs and applications to ensure output is consistent with expected content and format and quickly identify any anomalies.
14. Protect system memory by implementing data execution protection controls to prevent unauthorized executions in non-executable regions of memory or in prohibited memory locations.
15. Document and implement fail-safe procedures upon the failure of critical systems and operational components (e.g., communications failures. Fail-safe methods include alerting operator personnel and providing specific instructions on subsequent steps to take.)
16. During the information lifecycle, validate any DCH confidential data's accuracy, relevance, timeliness, and completeness (including "Sensitive Information") and correct or remove any inaccurate, incorrectly de-identified, or outdated information.
    - Perform data tagging on personally identifiable information to support automating Sensitive Information's correction and deletion process.
    - Collect Sensitive Information directly from the individual to ensure accuracy.
    - Correct or delete Sensitive Information upon request from the individual or their designee.
    - Notify the impacted individual and delegated authority when Sensitive Information has been deleted or corrected.
17. De-identify Sensitive Information in datasets by removing the association between a set of identifying data and the data subject by masking, encrypting, or replacing with dummy data for all non-live or transactional environments (including test, development QA, UAT, etc.).
    - De-identify upon collection if the data is not going to be used.
    - Do not perform archiving on Sensitive Information if the data will not be needed upon archiving.
    - Before releasing a dataset or data, the Data Custodian shall remove or de-identify Sensitive Information if that data is not considered necessary.
    - When performing statistical analysis, manipulate the numerical data, the analysis results, and tables so that an individual's identity cannot be inferred from the results.
    - Add non-deterministic noise to mathematical operations and algorithms before the results are reported to prevent the unintended disclosure of Sensitive Information.
    - Use only validated software and algorithms to perform de-identification of Sensitive Information.
    - Perform motivated intruder testing on de-identified datasets for attempting to re-identify an individual based on the remaining information.

18. Perform Data-Tainting to determine if data has been exfiltrated or improperly removed (e.g., embedding false data or email addresses and identify if that email address has been contacted or if the data appears in other sources).
19. Review Sensitive Information (and other DCH defined confidential information) on a case-by-case (as determined by the type of Sensitive Information and where hosted) basis for determining if the information is still required and delete as determined in alignment with DCH retention, contractual, and compliance requirements. Delete on-demand generated data when no longer needed.
20. Implement an Information Fragmentation program to divide information into disparate elements and distribute it across multiple systems and/or locations to reduce the risk of threats.

E. Definitions

- Data Custodian – An individual responsible for ensuring that the environment in which the data is stored complies with all applicable data security requirements, including establishing and maintaining security arrangements to prevent unauthorized use.
- Data Tainting – Analysis technique for finding bugs and vulnerabilities in software.
- DCH – Georgia Department of Community Health.
- De-Identified – Masking of data to prevent anyone's PII from being identifiable to a specific person.
- 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.
- Information Fragmentation – Threat management technique where information is divided and distributed across multiple systems to reduce the threat of unauthorized access and data exfiltration.
- MITF – Mean Time To Failure - Average amount of time that a part can run before it breaks.
- Motivated Intruder Testing – Analysis of de-identified Sensitive Information to determine if the individual can be identified based on available data.
- NIST - The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See https://www.nist.gov/.
- Non-Deterministic - A non-deterministic algorithm is one in which the outcome cannot be predicted with certainty, even if the inputs are known, while a deterministic algorithm always returns the same results given the same input.

- Non-Persistence – Data that is not available upon closing an application.
- 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.
- POAM - Plans of Action and Milestones, or a POAM, is a "document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones", as defined by NIST.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.
- SIEM – Security Information and Event Management – Automated methodology for capturing and analyzing logged events.
- SSP - System Security Plan that documents how an organization implements its security requirements and security guidelines and standards that the organization follows.
- Vulnerability - A security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered.

F. References: Please refer to NIST 800-53 Systems and Information Integrity (SI) Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for System and Information Integrity.

11/12/2023

Signature ***Date***