GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**547**	**Division:**	**Office of Information Technology**
Policy Title:	**Systems and Communications Protection (SC)**	**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 Systems and Communications Protection (SC) 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 Systems and Communications Protection (SC) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Systems and Communications Protection (SC) 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 Communications Protection (SC) 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 Communications Protection 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 Communications Protection policy and plan that addresses purpose, scope, roles, and procedures.
2. Ensure separation of user and system functionality (system management, e.g., DBAs, UNIX Root, Domain Admins) and restrict administrative privileges from ordinary users.
    - Store information about users' activities/interactions separately from application and software information.
3. Isolate security functions and information flow from non-security user functions.
    - Utilize hardware separation mechanisms (e.g., operator console)
    - Minimize or restrict the non-security functions within the isolation boundary containing the security functions.
    - Ensure that security modules are independent by maximizing internal cohesiveness within modules and minimizing coupling between modules.
    - Isolate security functions by implementing layered structures with minimized interactions between security functions.
4. Prevent unauthorized and unintended information transfer between shared systems.
5. Develop and implement controls to prevent and defend against Denial-of-Service (DOS) attacks.
    - Monitor to ensure sufficient performance and capacity to counter DOS flooding attacks and continue critical services.
    - Implement and deploy monitoring and alerting tools to detect DOS attacks.
6. Protect resources (capacity and performance) by allocating priorities and quotas to prevent lower-priority processes and services from using disproportionate resources and interfering with or preventing higher-priority services from running.
7. Ensure that communications are monitored and controlled at the external interfaces to the system and connections to external networks take place through these managed interfaces.
    - Implement subnetworks for publicly accessible systems that are logically separated from DCH internal networks with DMZs.
    - Restrict and control the number of external connections to DCH internal networks (Refer to the Trusted Internet Connection Initiative for guidance).
    - Implement a managed interface for the following:
        - Each telecommunication service.

        - Traffic flow policy and document each exception with a business justification and review each exception to ensure that the circumstances still apply.
        - Implement confidentiality and integrity protection for all information transmitted across each interface.
        - Manage and restrict control plane traffic from unauthorized exchanges with external networks and enable remote networks to detect unauthorized traffic.
    - Deny network communications by default and allow by exception at managed interfaces. Detect and deny suspect inbound and outgoing communications traffic to external sites and identify those internal users whose actions were denied.
    - Prevent split tunneling from remote devices unless the split tunnel can be securely provisioned using a Virtual Private Network (VPN) or other secured methodologies.
    - Use proxy servers to route communication traffic for clients requesting system resources (e.g., files, web pages) from non-organizational or other organizational servers.
    - Prevent and test against the exfiltration and leakage of data.
    - Only allow incoming communications from trusted and/or authorized sources.
    - Implement host-based boundary protection methodologies (e.g., host-based firewalls) to isolate system components.
    - Separate subnets from critical operations, configurations, and security components.
    - Deploy controls to protect against unauthorized physical access.
    - Route privileged remote user access through a dedicated managed interface.
    - Do not publish network addresses and periodically change them to prevent discovery.
    - Utilize system components that enforce protocol formats.
    - Maintain boundary protection devices at managed interfaces in the event of operational failure.
    - Deploy the ability to partition certain system components from other components.
    - Separate systems into subnetworks to ensure the appropriate level of protection to different security domains is applied and to isolate critical system functions.
    - Ensure that feedback to senders on protocol format validation failures is disabled.
    - For systems processing sensitive information, ensure that external interfaces to the system and at key internal boundaries within the system are monitored and;
        - Each processing exception is documented, reviewed, and removed when no longer needed.
    - Prohibit direct connection to public networks or external systems without boundary protection devices.
8. Protect the confidentiality and integrity of transmitted information on external and internal networks by:

- Implement cryptography to protect against and detect changes to information during transmission and maintain the protection during transmission preparation.
- Implement cryptographic mechanisms (e.g., concealing and randomizing communication patterns) to protect against the accidental disclosure of information.

9. Terminate network sessions and connections after an inactivity period of 15 minutes.
10. Provide an isolated trusted path between the users and trusted system components that the users and system components can activate.
11. Establish and manage a cryptographic key management program and maintain information (e.g., key escrow) in case of a lost key. (Forgotten passphrase).
    - Maintain control over the proliferation and distribution of asymmetric cryptographic keys.
    - Maintain physical control over cryptographic keys when encrypted information is stored on external systems (e.g., cloud provider).
12. Identify and document the cryptographic method used and how the program is managed.
13. Prohibit the remote activation of collaborative computing devices and implement a means to disconnect from such devices.
    - Provide the means to disable or remove collaborative devices from systems.
14. Link and verify the integrity of privacy and security attributes with the information exchanged between systems and components.
    - Implement anti-spoofing measures to prevent the falsification of security attributes.
    - Implement cryptographic (or other) mechanisms to bind privacy/security attributes.
15. Issue public key certificates in alignment with DCH policies and practices and obtain certificates from only approved providers.
    - Include only approved trust anchors in certificate stores managed by DCH.
16. Define, document, and implement a standardized process for authorizing, managing, monitoring, and using mobile code. Note: Mobile Code is not allowed by DCH.
    - Identify the criteria for unacceptable mobile code and the actions to be taken when such code is identified and prevent the downloading and execution of unauthorized or unacceptable mobile code.
    - Ensure that mobile code's acquisition and development align with DCH requirements and standards.
    - Prevent the automatic execution of mobile code (e.g., disabling auto-exec features).
    - Allow the execution of mobile code in dedicated and isolated environments to prevent the introduction of malicious software.
17. Provide data origin authentication and integrity verification in response to external queries and for internal name/address resolution queries.
18. Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
19. Ensure that systems are fault tolerant and implement internal and external role separations.

20. Protect communications session authenticity.
    - Invalidate session identifiers upon user logout or other session termination.
    - Generate a unique system identifier for each session and recognize only that.
21. Only allow the use of trusted certificate authorities for protected session establishment verification.
22. Fail to a known safe state for a set of events to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of systems or components or compromise.
23. Deploy system components with minimal functionality to reduce the exposure to threats and attacks.
24. Deploy the use of decoys (e.g., honeypots) and concealment and misdirection techniques to deflect attacks away from operational systems and high-value targets.
    - Deploy the concept of randomness to potentially confuse attackers.
25. Utilize platform-independent applications that can execute and are portable across multiple platforms to better ensure the availability of mission-critical applications if a system is under attack.
26. Protect the confidentiality, integrity, and availability of information at rest (stored) through controls.
    - Implement cryptographic mechanisms to prevent the unauthorized disclosure, access, and modification of information**.**
    - Identify and document the information to be removed from on-line storage and store offline.
    - Ensure that cryptographic keys are securely stored.
27. Deploy diverse information technologies to protect against and reduce the impact of failures and compromise.
28. Change virtual operating systems or applications, as opposed to changing actual operating systems or applications, to protect against attacks and failures and assist in the isolation of potentially malicious software.
29. Perform covert channel analysis (and estimate the bandwidth of channels) to prevent an attack that transfers information between processes that should be prevented from communicating by the existing policy.
    - Test identified covert channels to determine how they can be exploited.
    - Measure and eliminate as much of the bandwidth as possible without impacting performance.
30. Implement system partitioning as a means to physically or logically separate system components as a defense strategy.
    - Placed privileged functions in a separate physical partition to eliminate the risk of a single point of failure.
31. Deploy non-modifiable read-only storage to ensure data integrity and disallow the insertion of malicious code from the point of creation to insertion into the operating system and following the placement.
32. Implement methodology to identify network-based malicious code or malicious websites.
33. Distribute processing across multiple physical and logical domains to provide redundancy and overlap of functionality.

- Implement a process to identify potential faults, compromises, or errors in the distributed processing and storage components and the corrective actions to remediate the issues.
- Synchronize redundant and overlapping services to utilize the most current information when needed.

34. Utilize out of band channels for data backups; configuration management changes for hardware, firmware, or software; security updates; maintenance information; and malicious code protection updates and other non-routine operations traffic.
    - Deploy techniques to ensure that only authorized individuals and systems receive information (e.g., government issued identification).
35. Deploy operational security controls to protect information by:
    - Identifying critical systems.
    - Analyzing threats and vulnerabilities.
    - Assess Risks.
    - Apply remediation measures.
36. Isolate processes by maintaining separate processing domains through hardware separation mechanisms and separate domain threads.
37. Ensure that internal and external wireless links are protected from signal parameter attacks and the identification of wireless transmitters.
    - Implement cryptographic mechanisms to protect wireless networks against attacks and detection.
    - Deploy cryptography to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters**.**
38. Disable, disconnect, or remove any unnecessary connection ports or input/output devices to prevent the introduction of malicious code or malware.
39. Restrict or prohibit the use of sensor capabilities that can collect and record data regarding the environment where the system is in use.
    - Ensure the system is configured so that collected information is only sent to authorized individuals.
    - Ensure individuals are aware when sensors collect information about them and that the minimum amount of unneeded information is collected.
40. Establish and document usage restrictions for designated system components.
    - Authorize, justify, monitor, and control such usage.
41. Utilize an isolated or dedicated environment (detonation chamber) to execute untrusted functions in a sandbox or non-networked environment to identify malicious code or malware and prevent propagation.
42. Synchronize time clocks between systems and components to an authoritative time source.
    - Identify/deploy a secondary time source if the primary authoritative time source is unavailable.
43. Implement cross domain policy enforcement to prevent the ability to bypass an enforcement.
44. Identify and deploy alternative communication paths to be used in the event that the established communication path is disrupted due to an incident.

45. Monitor and relocate sensors and alerting/monitoring capabilities under disaster/incident recovery circumstances to detect threats and deter service attacks and disruptions.
46. Implement software enforced separation and policy enforcement to ensure domain separation and deter threats.
47. Implement write-protect for hardware and the capability to both manually disable write-protect during modifications/upgrades, etc., and reinstate following a return to normal operations.

E. Definitions

- Asymmetric Cryptographic Keys – Utilizing one public key and one private key to encrypt and decrypt.
- Cohesion – The class is focused on what it should be doing (e.g., security functions),
- Coupling – The relationship or dependency of two classes toward each other.
- DCH – Georgia Department of Community Health.
- De-Identified – Masking of data to prevent anyone's PII from being identifiable to a specific person.
- DOS - Denial-of-Service - A deliberate attempt by an unauthorized party to crash services or flood services (slowing down the service).
- 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).
- Fault Tolerant – A system's ability to operate uninterrupted despite component failure.
- 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.
- In Band Channel – Sending data through the same band and channel that is only used for data transmission.
- NIST - The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See https://www.nist.gov/.
- Out of Band Channel – An independent channel allowing data to be transmitted separately from in Band Channels.
- 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.
- Split Tunneling - Allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network.
- SSP - System Security Plan (NIST 800-18 Appendix A SSP format) 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.
- Fault Tolerant – A system's ability to operate uninterrupted despite component failure.

F. Please refer to NIST 800-53 Systems and Communications Protection (SC) Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Systems and Communications Protection.

November 29, 2023

Signature ***Date***