GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**546**	**Division:**	**Office of Information Technology**
Policy Title:	**Systems and Services Acquisition (SA)**	**Effective Date:**	**November 21, 2024**
Version:	**2**	**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 Services Acquisition (SA) 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 Services Acquisition Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Systems and Systems and Services Acquisition 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 Services Acquisition 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 Services Acquisition 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 this Systems and Services Acquisition policy and procedure and manage the program.

D. The Systems and Services Acquisition policy shall be reviewed annually to ensure its continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy shall be updated to reflect changes in relevant factors, such as technology, regulations, or internal practices. The revised policy shall be communicated to all affected parties.

E. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Systems and Services Acquisition policy and plan that addresses purpose, scope, roles, and procedures.
2. Identify, document, and allocate the resources needed to protect the system when determining the information security and privacy requirements for the system and service being considered.
    - Designate information security and privacy as a discrete budgetary line item.
3. Develop and implement a System Development Lifecycle (SDLC) Plan incorporating privacy and security considerations.
    - DCH shall define, document, and identify information privacy and security roles and responsibilities throughout the SDLC.
    - Integrate the Risk Management program into the SDLC activities.
    - Apply commensurate system level protection throughout the pre-production (development, test, integration, and QA) phases.
    - Restrict, approve, and document the use of live data throughout the pre-production phases.
    - Apply the same Data Security Categorization levels during the pre-production phases as would be applied to systems pre-production.
    - Develop and implement a technology refresh (update) methodology and schedule during the SDLC.
4. Implement and document an acquisition process that incorporates the following areas:
    - Functional, privacy/security, and assurance requirements plus needed controls to address requirements.
    - Plan to protect privacy and security documentation (e.g., least privilege, roles based, storage, etc.)
    - Defined information and privacy security roles and responsibilities within supply chain management.
    - Description of the environments (e.g., development, test) in which the system is to operate.
    - Definition of acceptance criteria.

- Develop documentation of the control properties to be implemented.
- Require the developer to provide design and implementation information for the system and identify functions, ports, protocols, and services intended for organizational use. as well as the SDLC plan for testing, evaluation, assessment, QA, and acceptance.
- Ensure that the developer uses and delivers the configuration baseline for new systems, replacements, reinstalls, upgrades, etc.
- Limit the use of commercially acquired products and services to those that, through evaluation, meet National Information Assurance Partnership (NIAP) standards. If NIAP does not apply**,** the product relies on cryptographic functionality to enforce its security policy that the cryptographic module is validated by Federal Information Processing Standards (FIPS) or National Security Agency-approved**.**
- Developers must implement a continuous monitoring program of services and systems to validate control effectiveness.
- Ensure the systems and services acquisition contract includes all privacy and data ownership requirements. The contract should also include when data is removed and returned to DCH from the contractor's systems.

5. Develop or obtain system or service administrator documentation for the proposed product that includes:
   - Secure configuration, installation, and operation of the system, component, or service.
   - Usage of security and privacy functions.
   - Known vulnerabilities and using privileged users (e.g., system admins, access admins, DBAs, etc.).
   - User accessible security and privacy functions and how to use them (e.g., self-service password resets).
   - How individuals would use the system in a more secure manner.
   - User security and privacy related responsibilities.
6. Apply the systems security and privacy engineering principles below to ensure the development of secure and resilient systems that can better defend against threats and vulnerabilities.
   - Implement a well defined and clear security design that embodies the following principles:
     - Least Common Mechanism, Modularity, and Layering,
     - Partially Ordered Dependencies Efficiently Mediated Access,
     - Minimized Sharing, and Reduced Complexity,
     - Secure Evolvability and Hierarchal,
     - Protection Trust and Trusted Components,
     - Inverse Modification Threshold,
     - Minimized Security Elements, and Least Privilege,
     - Predicate Permission, and Self-Reliant Trustworthiness,
     - Secure Distributed Composition, and Continuous Protection,
     - Secure Metadata Management, Self-Analysis, Accountability and Traceability,

        - Secure Defaults, Secure Failure, and Recovery, Repeatable Documented Procedures, and Procedural Rigor,
        - Secure System Modification, sufficient documentation, and Minimization Privacy Principle,
        - Economic, Performance, and Human Factor Security,
7. Require that Service Providers comply with DCH security and privacy requirements.
    - Define, document, and implement roles responsible for oversight of Service Provider compliance and monitoring on an ongoing basis.
    - Conduct a risk assessment before acquiring or outsourcing systems and/or services or signing a contract.
    - Ensure that the CISO has approved the acquisition or outsourcing of the systems and services.
    - Service Providers must provide their system protocols, ports, defaults, and other required services.
    - Establish, document, maintain, and monitor trust relationships between DCH and external Service Providers.
    - Ensure that due diligence is performed before establishing a business relationship with an external Service Provider to ensure their values are consistent with DCHs.
    - Define restrictions on services, processing, and storage with the external Service Provider.
    - Define with the vendor that DCH shall maintain control of cryptographic keys for encrypted material used, stored, or transmitted by the external Service Provider.
    - Restrict the geographic storage and processing to Service Provider facilities within the jurisdiction of the United States.
8. Ensure that developers maintain systems configuration management during design, development, testing, implementation, operation, and disposal.
    - Developers shall implement only DCH approved changes and maintain data integrity throughout the lifecycle.
    - Developers shall document approved changes and note the security impact of such changes.
    - Developers shall track and report all security flaws up to and including resolution.
    - Enable integrity checking mechanisms on hardware, software, and firmware.
    - Implement an alternative configuration management process to review commercial off-the-shelf products where in house development does not take place.
    - The developer shall deploy the use of tools to compare previous versions of source code and object code to modified versions to verify and monitor authorized changes to hardware, software, and firmware.
    - The developer shall maintain the integrity mapping of the master build data describing the current security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

- The developer shall implement and deploy procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies**.**
- Ensure that security and privacy representation are included in configuration change management and planning.

9. Developer shall execute the below testing and evaluation tasks:
    - Document and implement a plan for performing ongoing security and privacy assessments and maintain results and evidence of assessments. An independent (external) party shall be provided the appropriate information and validate the plan was implemented and executed correctly.
    - Performing integration, regression, QA, and unit testing at appropriate frequencies and points in the process.
    - Implement a verifiable flaw remediation process and document/correct identified flaws, employ dynamic code analysis tools to identify common flaws and document the analysis results, and employ interactive application security testing tools to identify flaws and document the results.
    - Utilize static code analysis tools to identify common flaws and document the analysis results.
    - Perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of phases.
    - Perform a manual code review on critical systems and components.
    - Perform external penetration testing for Medicaid systems before production.
    - Perform attack surface reviews and reduce the attack surface risks identified.
    - Verify that the testing and evaluation scope covers the required controls completely.
10. Developers shall follow a documented and implemented process that includes:
    - Security and privacy requirements and review of the processes, tools, and configurations to ensure that requirements are being met.
    - Development tools and tool configurations are utilized in the development process.
    - Documents, managers, and monitors change integrity.
    - Define metrics and standards early in the development process and how those will be measured and reported.
    - Utilize security and privacy tracking tools during the development process and criticality analysis for high level assets.
    - Define criteria for continuous monitoring and improvement of the development process.
    - Perform and report on automated vulnerability analysis and risk mitigation strategies, as well as use threat modeling and vulnerability analyses from similar software and systems to inform of potential issues.
    - Retain key development artifacts and evidence by archiving the system component to be released or delivered and maintaining the evidence and the baseline for available reference.
    - Document, implement, and test an Incident Response Plan.
    - Minimize the use of personally identifiable information in development and test environments.

11. Provide training on the operation of the system or service to ensure the effectiveness of the implemented security and privacy controls.
12. The developer shall produce a formal policy model and design specifications aligned with security and privacy architecture in alignment with DCH security and privacy architecture that addresses the physical and logical controls and requirements and:
    - Addresses how security and privacy functions work together to ensure adequate protection.
    - Develop relevant and verifiable security software, hardware, firmware, and interfaces that specify exceptions, error messages, and effects and align with DCH security and privacy requirements.
    - Develop the hardware, software, and firmware with reduced complexity to reduce the risk of introducing vulnerabilities.
    - Promote complete, concise, consistent, and comprehensive testing and evaluation of systems, software, and firmware being developed.
    - Ensure that each system, software, and firmware are configured to support the concept of least privilege.
    - Coordinate security resources to ensure consistent security configuration changes or updates (e.g., patching) are uniformly applied.
    - Employ design diversity (e.g., utilizing different developers with different experiences in development) in system and software development against a common set of specification requirements.
13. Custom develop or re-do system components determined to be vulnerable or have no or inadequate security controls to mitigate risk.
14. Perform personnel screening on developers in alignment with Insider Threat criteria.
15. Develop and implement a plan to retire or replace vendor unsupported or obsolete systems and components.
    - Develop a plan for alternative methods to maintain and support a system the vendor no longer supports until the system can be replaced or retired (e.g., in-house support and development).
16. Develop a method to customize or augment system components that support mission-critical functions to enhance the trustworthiness or security during the design or post-design.

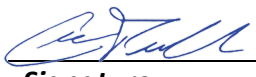
F. Definitions

- Acceptable Security – Privacy, security, and performance levels meet the user's expectations.
- Accountability and Traceability – Trace an action to an individual.
- DCH – Georgia Department of Community Health.
- Economic Security – The cost of implementing security controls does not exceed the cost of damage incurred from not implementing the controls.
- 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).

- FIPS – Federal Information Processing Standards – NIST developed government standards for non-military American government computing agencies.
- FISMA - Federal Information Security Modernization Act
- Hierarchal Protection – The system's security operates at the level of the highest security component of the system.
- 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.
- Human Factor Security - User security interfaces are clear and provide feedback and warning to users when an insecure choice is made (e.g., invalid login attempt).
- Inverse Modification Threshold – The degree of protection to a component is commensurate with its trustworthiness.
- Layering – Simple understood dependencies between units
- Least Common Mechanism - The number of mechanisms common to more than one user and dependent on all users is minimized (different components refrain from using the same method to access system resources).
- Least Privilege – The minimum amount of access necessary to perform a given function.
- Minimization Privacy Principle – PII should only be processed when necessary and should be minimized.
- Minimized Security Elements – Minimizing the cost and complexity of security analysis.
- MTTF (Mean Time To Failure) - Average amount of time that a part can run before it breaks.
- Modularity - Function Isolation
- Motivated Intruder Testing – Analysis of de-identified Sensitive Information to determine if the individual can be identified based on available data.
- National Information Assurance Partnership (NIAP) – to ensure that acquired systems and services meet security competence requirements.
- NIST - The National Institute of Standards and Technology as part of the US 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.
- Partially Ordered Dependencies – Layers are structured so that higher layers are dependent on lower layers.
- PII – Personally Identifiable Information - PII is defined by the 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 USC 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.
- Predicate Permission – To support separation of duties, multiple authorizing functions must approve prior to access sensitive data or performing sensitive operations.
- Procedural Rigor – The scope, depth, and detail of the system life cycle procedures.
- QA (Quality Assurance) – Evaluation of product to ensure production readiness.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.
- SDLC (System Development Lifecycle) – The phases of planning, developing, testing, and implementing systems and software.
- Secure Defaults – Deny All by policy default; access must be explicitly granted.
- Secure Distributed Composition - The system enforces the policy in the same way for distributed components as it does for individual components.
- Secure Evolvability – Developing a system to ensure the maintenance of its security properties during upgrades and changes.
- Secure Failure and Recovery – System failures and recovery do not lead to a violation or degradation of security policies.
- Secure Metadata Management – Protecting data that describes and provides information about other data.
- Secure System Modification – Security is maintained during system modifications.
- Self-Analysis – A system component can assess its internal state and functionality.
- Self-Reliant Trustworthiness – Systems do not rely on other systems to establish their own trustworthiness.
- SSP - System Security Plan that documents how an organization implements its security requirements and security guidelines and standards that the organization follows.
- Trusted Components - Trust relationship that a component is as trustworthy as the security dependencies supported.
- Trusted Communications Channels - Each communications channel is trustworthy commensurate to the security dependencies it supports.
- 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.

G. References: Please refer to NIST 800-53 Systems and Services Acquisition (SA) Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for System and Services Acquisitions.



11/22/2024

Signature ***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	11/21/2024	• Added a revision history table to validate consistent review/update and document changes • Section D: The policy shall be reviewed annually	DCH CISO