	System and Services Acquisition Policy		**Document No.** SCIO-SEC-315
Effective Date 01/29/2018	**Review Date** 03/26/2025	**Version** 4	**Page No.** 1 of 14

Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law. This security policy is consistent with applicable laws, executive orders, directives, regulations, other policies, standards, and guidelines.

Material Superseded

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

Responsibilities

All covered personnel involved in the acquisition, development or operation of information systems and supporting infrastructure are responsible for adhering to this policy and with any local system and service acquisition requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for documenting, disseminating and implementing a secure information system and service acquisition program throughout the agencies.
Agency Security Liaison	The Agency Security liaison(s) are responsible for ensuring that information system and service acquisition requirements are managed in compliance with the State's requirements by collaborating with organizational entities. Liaison(s) are responsible for maintaining the appropriate information system and service acquisition requirements required for information security protection.
Information System Owner	The Information System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Third Parties	Third party service providers are responsible for implementing secure information systems, system components, and services.

SA-1 – Policy and Procedures

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document provides requirements for the system and service acquisition process which is required to assure that information systems are acquired using controls sufficient to safeguard the State's information systems. This document addresses the requirements set forth by the State to implement the family of System and Service Acquisition security controls at the organization, process and/or system level for all information assets / State data. Failure to protect network infrastructures against threats can result in the loss of data integrity, loss of availability of data, and/or unauthorized use of data or information systems of which State agencies are considered the owner.

The State has adopted the System and Service Acquisition principles established in National Institute of Standards and Technology (NIST) SP 800-53 "System and Service Acquisition" control guidelines as the official policy for this security domain. The "SA" designator identified in each control represents the NIST-specified identifier for the System and Service Acquisition control family. The following subsections in this document outline the system and service acquisition requirements that each agency must implement and maintain adhere to in order to be compliant with this policy.

This policy and associated procedures shall be reviewed and updated annually, at a minimum. They shall also be updated following agency-defined events that necessitate such change.

This policy and the associated procedures shall be developed, documented, and disseminated by the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

SA-2 – Allocation of Resources

Organizations shall expediently allocate resources for information security to provide rapid yet supervised allocation, ensuring that the organization is modernized and protected against emerging and ongoing threats. Funding shall include allocation of resources for the initial system or system service acquisition, and funding for the sustainment of the system/service. The following items shall be done:

a. Determine the high-level security and privacy requirements for the system or service in each mission or business-process planning.

b. Identify, document, and allocate the appropriate amount of resources which are required to protect the system or service as part of the capital planning and investment control process.

c. Establish discrete line items for information security and privacy in the budgeting process.

SA-3 – System Development Life Cycle

Organizations shall acquire, develop, and manage systems using a System Development Life Cycle (SDLC) that incorporates information security and privacy considerations:

a. Identify qualified individuals having information security and privacy roles and responsibilities that are involved in creating the SDLC. This may include the CIO, CISO, business owners, system administrators, security architects, security engineers, security analysts, etc. These personnel will ensure that the system life cycle activities meet the security and privacy requirements for the organization.

b. Define and document information security and privacy roles and responsibilities throughout the SDLC.

c. Integrate the agency information security and privacy risk management process into SDLC activities.

d. A business case justification of custom system development projects shall be required. When proposing the development of custom software, a strong business case shall include the following:

   i. Support the rationale for not enhancing current systems;

   ii. Demonstrate the inadequacies of packaged solutions; and

   iii. Justify the creation of custom software.

e. The organization shall implement a change management program which enables system engineers, architects, and security analysts to expediently perform their necessary business functions, yet maintain a controlled, secure, and functioning environment. Examples of this program include multi-tiered deployments (Dev, Test, Quality Assurance (QA), Production), which are capable of backing-up and rolling-back changes which are unsuccessful. Change control requirements are provided in the Configuration Management Policy, SCIO-SEC-305, Section CM-3.

f. The organization will plan for End-of-Life (EoL) and End-of-Support dates (EoS) for systems and services. This will ensure that systems and services can receive security patches and updates throughout the system development lifecycle, and that the organization is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured. See also CM-2 Baseline Configuration for more information about supported versions of products.

GUIDELINES

a. Many SDLC models exist that can be used by an organization in developing an information system. A traditional SDLC is a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle. A general SDLC should include the following phases:

i. Initiation

ii. Acquisition / Development

iii. Implementation / Assessment

iv. Operations / Maintenance

v. Sunset (disposition)

b. Each of these five phases should include a minimum set of tasks to incorporate security in the system development process. Including security early in the SDLC will usually result in less expensive and more effective security than retrofitting security into an operational system.

c. The following questions should be addressed in determining the security controls that will be required for a system:

i. How critical is the system in meeting the organization's mission?

ii. What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?

iii. What regulations, statutes, and policies are applicable in determining what is to be protected?

iv. What are the threats that are applicable in the environment where the system will be operational?

v. What kinds of data will be used by the system?

SA-4 – Acquisition Process

Security functional requirements are a part of the hardware, software, or firmware acquisition process. Agencies shall be capable of acquiring necessary solutions in an expedient manner in accordance with N.C.G.S. 143B-1350., The following shall be done.

a. Security and privacy functional requirements shall include security capabilities, security functions, and security mechanisms.

b. Strength of mechanism requirements based on security categorization, e.g., Low or Moderate, associated with such capabilities, functions, and mechanisms shall include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass.

c. Security and privacy assurance requirements shall include the following:

i. Development processes, procedures, practices, and methodologies;

ii. Evidence from development and assessment activities providing grounds for confidence that the required security and/or privacy functionality has been implemented and the required security strength has been achieved.

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements.

f. Requirements for protecting security and privacy documentation.

g. Description of the information system development environment and environment in which the system is intended to operate.

h. Acceptance criteria requirements for assessing the ability of a system component, software or system to perform its intended function.

i. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.

j. Proposed vendor hardware design shall comply with information security and other State policies and standard security and technical specifications, such as the following:

   i. Vendors shall configure the system with adequate capacity to fulfill the functional requirements stated in the agency's design document.

   ii. Vendor shall configure hardware security controls to adequately protect data. (Optionally, the vendor may assist the agency with the configuration of software security controls to provide adequate data protection on the vendor's hardware.)

k. Systems under consideration for acquisition shall be interoperable with the peripherals and systems currently in use.

l. To mitigate risks of exploitation of covert channels third-party applications shall be obtained from reputable sources.

m. Non-security functional and technical requirements shall be a part of the hardware, software, or firmware acquisition process.

n. Agencies shall follow State procurement policies when acquiring hardware to ensure that the purchase meets specified functional needs. Agencies shall include specific requirements for performance, reliability, cost, capacity, security, support, and compatibility in Requests for Proposals (RFPs) to properly evaluate quotes.

o. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval. This document is intended to help agencies reach a decision for a specific system that will meet the State's security and compliance requirements. A VRAR is required for both solutions hosted on State infrastructure and those that are not hosted on State infrastructure.

p. New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the agency.

SA-4 (1) – Acquisition Process | Functional Properties of Controls

Developer(s) of the system, system component, or information system service shall provide a description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality (e.g., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

SA-4 (2) – Acquisition Process | Design and Implementation Information for Controls

Developer(s) of a system, system component, or information system service shall provide design and implementation information for the security controls to be employed that includes the following: security-relevant external system interfaces, high-level design, source code, or hardware schematics.

SA-4 (9) – Acquisition Process | Functions, Ports, Protocols, and Services in Use

Developer(s) of a system, system component, or information system service shall identify the functions, ports, protocols, and services intended for use.

SA-4 (10) – Acquisition Process | Use of Approved PIV Products

Information technology products on the FIPS 201-approved products list shall be employed for Personal Identity Verification (PIV) capability implemented within agency systems.

SA-5 – System Documentation

Organizations must obtain, develop, or document administrator and user documentation for the system, system component, or system service. Such documentation shall be distributed to designated agency officials that describes the following:

a. Secure configuration, installation, and operation of the system, component, or service.

b. Effective use and maintenance of security and privacy functions/mechanisms.

c. Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.

d. User-accessible security and privacy functions/mechanisms and how to effectively use those functions/mechanisms.

e. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.

f. What responsibilities the end user has in maintaining the security and privacy of the individuals.

The following shall also be done:

g. Ensure each new or updated system includes supporting system documentation and technical specifications of information technology hardware, whether the system is developed or updated by in-house staff or by a third-party vendor.

h. Create, manage, and secure system documentation libraries or data stores that are always available to only authorized personnel.

i. Ensure that system documentation is readily available to support the staff responsible for operating, securing, and maintaining new and updated systems.

j. Control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting and staff turnover.

k. All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.

SA- 6 – Software Usage Restrictions

Withdrawn: Incorporated into CM-10 and SI-7.

SA-7 – User Installed Software

Withdrawn: Incorporated into CM-11 and SI-7.

SA-8 – Security and Privacy Engineering Principles

Organizations shall apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. Security and Privacy engineering principles shall be primarily applied to new development information systems or systems undergoing major upgrades. For legacy systems, organizations shall apply security engineering principles to system upgrades and modifications to the extent that it is technically configurable, given the current state of hardware, software, and firmware within those systems.

a. Security and Privacy engineering principles shall include the following:

   i. Developing layered protections;

   ii. Establishing sound security and privacy policy, architecture, and controls as the foundation for design;

   iii. Incorporating security and privacy requirements into the SDLC;

iv. Delineating physical and logical security boundaries;

v. Ensuring that system developers are trained on how to build secure software;

vi. Tailoring security and privacy controls to meet organizational and operational needs;

vii. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;

viii. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

b. NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems shall be used as guidance on engineering principles for information system security. NIST SP 800-160 may be found at the following link:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

c. This control is optional for LOW risk information systems.

SA-9 – External System Services

Agencies shall require that third parties and providers of external system services comply with statewide information security and privacy requirements. Agencies shall employ controls as follows:

a. Define and document how external information system comply with statewide information security and privacy controls to include user roles and responsibilities and compliance auditing and reporting requirements. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval.

b. Monitor security and privacy control compliance by external service providers on an ongoing basis.

c. Restrict the location of information systems that receive, process, store, or transmit state and federal data to areas within the following areas:

i. US States,

ii. US Territories,

iii. US Embassies,

iv. US Military installations (stateside or overseas)

d. Agencies that outsource their information processing must ensure that the service provider demonstrates compliance with state standards and procedures, and industry quality standards.

e. Outsourcing agreements shall include the following:

i. The agency's course of action and remedy if the vendor's security and privacy controls are inadequate such that the confidentiality, integrity or availability of the agency's data cannot be assured.

ii. The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters.

iii. The vendor's ability to provide processing in the event of failure(s).

f. To support service delivery, the outsourcing agreements shall contain, or incorporate by reference, all the relevant security and privacy requirements necessary to ensure compliance with the statewide information security standards, the agency's record retention schedules, its security policies, and its business continuity requirements.

g. Services, outputs, and products provided by third parties shall be reviewed and checked, at minimum annually, in accordance with state statutes.

i. To monitor third party deliverables, agencies shall do the following:

a) Monitor third party service performance to ensure service levels meet contract requirements.

b) Review reports provided by third parties and arrange regular meetings as required by contract(s).

c) Resolve and manage any identified problem areas.

j. Contracts with vendors providing offsite hosting or cloud services that will host Restricted or Highly Restricted data must require the vendor to provide the State an independent, third-party risk assessment report (e.g., Service Organization Control (SOC) 2 Type II, International Organization for Standardization (ISO) 27001:2022, Federal Risk and Authorization Management Program (FedRAMP) Moderate), or HITRUST CSF (Common Security Framework)) before contract award and annually thereafter to establish compliance with state policy.

k. Any changes to services provided by a third party must be approved by the agency prior to implementation.

l. Agencies shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data.

m. Agencies shall ensure that the service-level agreement (SLA) includes requirements for regular monitoring, review, and auditing of the service levels and security requirements as well as incident response and reporting requirements. The SLA shall state how the service provider is responsible for data stored or shared with the provider.

n. Agencies shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. Agencies shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level.

o. Changes to an SLA and services provided shall be controlled through formal change management.

p. Agencies must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit Highly Restricted data, including federal tax information (FTI), unless explicitly approved by the Office of Safeguards.

SA-9 (2) – External System Services | Identification of Functions/Ports/Protocols/Services

Providers of external system services shall identify the functions, ports, protocols, and other services required for the use of such services. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.

SA-10 – Developer Configuration Management

System developers shall create and implement a configuration management plan that does the following:

a. Performs configuration management during system design, development; implementation, operation and/or disposal for the following:

   i. Internal system development and system integration of commercial software;

   ii. External system development and system integration;

b. Documents, manages, and controls changes to the system or configuration items; and the potential security and privacy impacts

c. Implements only agency approved changes to the system,

d. Documents approved changes to the system,

e. Tracks security flaws and flaw resolution within the system,

f. Organizations shall mitigate risks of exploitation of covert channels by protecting the source code in custom developed applications.

SA-11 – Developer Testing and Evaluation

System developers shall test for software faults that pose a security risk at all post-design stages of the system development life cycle prior to putting an application into production. The following shall be done:

a. Develop and implement a security and privacy assessment plan;

i. Develop and implement a plan that supports ongoing security and privacy assessments. Testing requirements must be defined and documented for both system development and system integration activities. The plan must include requirements for retesting after significant changes occur.

ii. Perform security testing/evaluation.

1. Restricted or Highly Restricted data shall not be used for testing purposes.

2. Organizations may permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and policies. Data anonymization or data masking tools shall be used if available.

3. If production data is used for testing, the same level of security controls required for a production system shall be used.

iii. Produce evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation

iv. Implement a verifiable flaw remediation process

v. Correct flaws identified during security testing/evaluation

b. Teach and encourage software fault-reporting procedures through security training and awareness programs.

c. Designate a quality control team that consistently checks for faults and that is responsible for reporting them to software support.

d. Use a formal recording system for the following:

i. Tracks faults from initial reporting through to resolution.

ii. Monitors the status of reported faults and confirms that satisfactory resolutions have been achieved.

iii. Provides reports and metrics for system development and software support management.

iv. Software faults shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability

e. While faults are being tracked through to resolution, research shall also be conducted to ensure no security controls have been compromised and resolution activities have been appropriately authorized.

f. Perform unit, integration, and system regression testing/evaluation:

i. Require that information system developers/integrators perform a vulnerability assessment to document vulnerabilities, exploitation potential, and risk mitigations.

ii. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.

iii. To maintain the integrity of information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment.

iv. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment.

v. Qualified personnel must certify that the upgrade or change has passed acceptance testing.

vi. A rollback plan must be established in the event the upgrade or change has unacceptable ramifications.

g. The following issues and controls shall be included when developing acceptance criteria and acceptance test plans:

i. Capacity requirements - both for performance and for the computer hardware needed.

ii. Error response - recovery and restart procedures and contingency plans.

iii. Routine operating procedures - prepared and tested according to defined policies.

iv. Security controls - agreed to and put in place.

v. Manual procedures - effective and available where technically configurable and appropriate.

vi. Business continuity - meets the requirements defined in the business continuity plan.

vii. Impact on production environment - able to demonstrate that installation of new system will not adversely affect current production systems (particularly at peak processing times).

viii. Training - of operators, administrators, and users of the new or updated system.

ix. Logs - logs of results shall be kept for a defined period once testing is completed.

h. Implement a verifiable flaw remediation process to correct security weaknesses and deficiencies identified during the security testing and evaluation process.

i. Controls that have been determined to be either absent or not operating as intended during security testing/evaluation must be remediated.

j. This control is optional for LOW risk information systems.

SA-12 – Supply Chain Protection (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-13 – Trustworthiness (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-14 – Criticality Analysis (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-15 – Development Process, Standards, and Tools (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-15 (3) – Development Process, Standards, and Tools – Criticality Analysis (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-16 – Developer Provided Training (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-17 – Developer Security Architecture and Design (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-18 – Tamper Resistance and Detection (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-19 – Component Authenticity (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-20 – Customized Development of Critical Components (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-21 – Developer Screening (Optional)

This control is optional for LOW and MODERATE risk information systems.

SA-22 – Unsupported System Components

Agencies must replace system components, e.g., servers, workstations, laptops, applications, etc., when support for the components is no longer available from the developer, vendor, or manufacturer. Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.