DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

System and Service Acquisition Policy

Document No.
SCIO-SEC-315-00

Effective Date	Review Date	Version	Page No.
01/29/2018	2/21/2020	2	1 of 13

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.

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 and implementing secure information system and service acquisition practices 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

All agency information assets 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. 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 shall be reviewed annually, at a minimum.

SA-2 – Allocation of Resources

Agencies shall expediently allocate resources for information security, in order 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. Agencies shall accomplish this mission by doing the following:

a. Determine the security 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 systems or services within the budgeting process.

SA-3 – System Development Life Cycle

Agencies shall manage information systems using a SDLC that incorporates information security considerations:

a. Identify qualified individuals having information security 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 requirements for the organization.

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

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

d. Agencies shall require a business case justification of custom system development projects. When proposing the development of custom software, agencies shall make a strong business case that does the following:

   i. Supports the rationale for not enhancing current systems;

   ii. Demonstrates the inadequacies of packaged solutions; and

   iii. Justifies 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 Control, 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 are capable of receiving 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.

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?

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, and any other applicable state or federal laws, directives, policies, regulations, standards, guidelines, and business needs. Agencies shall ensure the following.

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

b. Security strength requirements based on security categorization, i.e. 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 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 functionality has been implemented and the required security strength has been achieved

d. Requirements for protecting security-related documentation.

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

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

g. Proposed vendor hardware design complies 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.)

h. Agencies should ensure that systems under consideration for acquisition are interoperable with the peripherals and systems currently in use.

i. Agencies shall mitigate risks of exploitation of covert channels by obtaining third-party applications from reputable sources and by protecting the source code in custom developed applications.

j. Agencies shall ensure that non-security functional and technical requirements are also part of the hardware, software, or firmware acquisition process.

k. 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.

l. 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 requirement is for both solutions hosted on State infrastructure and those that are not hosted on State infrastructure.

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

n. Agencies shall require developer(s) of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality (i.e., 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.

o. Agencies shall require developer(s) of an information system, system component, or information system service to 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.

p. Agencies shall require developer(s) of an information system, system component, or information system service to identify early in the SDLC, the functions, ports, protocols, and services intended for agency use.

SA-5 – Information System Documentation

Agencies must obtain, or document attempts to obtain, administrator and user documentation for the information system, system component, or information system service. Agencies shall distribute such documentation 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 functions/mechanisms

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

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

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

f. What responsibilities the end user has in maintaining the security of the system, e.g. password protection, sharing information, etc.

Agencies shall also do the following:

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 agency 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 Engineering Principles

Agencies shall apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems. Security 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 engineering principles shall include the following:

   i. Developing layered protections;

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

iii. Incorporating security 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 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 800-27, Revision A *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, shall be used as guidance on engineering principles for information system security. NIST SP 800-27 Rev. A may be found at the following link:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf

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

SA-9 – External Information System Services

a. Agencies shall require that third parties and providers of external information system services comply with statewide information security requirements and employ to include (at a minimum) security requirements contained in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements.

b. Agencies shall define and document how external information system comply with statewide information security 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.

c. Agencies shall monitor security control compliance by external service providers on an ongoing basis.

d. Agencies shall restrict the location of information systems that receive, process, store, or transmit state and federal data to areas within the United States territories, embassies, or military installations.

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

f. Outsourcing agreements shall include the following:

i. The agency's course of action and remedy if the vendor's security 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).

g. To support service delivery, the outsourcing agreements shall contain, or incorporate by reference, all the relevant security 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.

h. 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 must require the vendor to provide the State with an annual third-party risk assessment report (e.g. Service Organization Control (SOC) 2 Type II, International Organization for Standardization (ISO) 27001, Federal Risk and Authorization Management Program (FedRAMP) Moderate), to establish compliance with state statues. The assessment shall include, at a minimum, the following:

i. The rate of compliance with the enterprise-wide security standards;

ii. An assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security.

iii. Estimate the cost to implement the security measures needed for agencies to fully comply with the standards.

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 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 Information System Services – Identification of Functions/Ports/Protocols/Services (Moderate Control)

Agencies shall require providers of external information system services to 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

Agencies shall require the information system developer to create and implement a configuration management plan that does the following:

a. Performs configuration management during information system design, development; implementation, and operation 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 information system or configuration items under configuration management,

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

SA-11 – Developer Security Testing and Evaluation

Agencies shall require the information system developer to test for software faults that pose a security risk prior to being put into production. Agencies shall do the following:

a. Create and implement a security assessment plan;

i. Create and implement a security assessment plan. Testing requirements must be defined and documented for both information 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. Agencies 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. Agencies shall use data anonymization or data masking tools, if they are 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 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 agency 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. Agencies shall include the following issues and controls 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 agency 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 agency’s business continuity plan.

vii. Impact on production environment - able to demonstrate that installation of new system will not adversely affect agency’s 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 an agency 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-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 Component

Agencies must replace information system components (specifically security patches and/or product updates) when support for the components is no longer available from the developer, vendor, or manufacturer.

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.

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.

DocuSigned by:
Tracy Doaks
EEADAC04EB804A3...

Approved: ________________ 3/3/2020 | 11:17 AM EST

Secretary of Department of Information Technology (DIT)