DocuSign Envelope ID: 512C65D9-33EA-4DF8-AC77-1801BE7BE275

Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. They 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, and other policies, standards, and guidelines.

This policy document provides the State of North Carolina's (State) Supply Chain Risk Management policy statements and commitment to develop, implement, maintain reasonable supply chain assurance methods and practices to strategically manage supply chain risks over the life cycle of information systems, products, and services.

Material Superseded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 that are included in IT risk assessment activities are responsible for adhering to this policy and with any local Risk Assessment requirements.

Role	Definition
Senior Management	Senior Management (the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designating organizational official) is responsible for the sponsorship and support of the Supply Chain Risk Management Plan and process, the review and approval of risk assessments and control recommendations and reporting to the SCRO what mitigation actions have been taken.
State Chief Risk Officer	The State Chief Risk Officer (SCRO) as delegated by the State CIO is assigned the responsibility for the continued development, implementation, and maintenance of the risk management program.

DocuSign Envelope ID: 512C65D9-33EA-4DF8-AC77-1801BE7BE275

Risk Management	The Enterprise Security and Risk Management Office (ESRMO) is responsible for governing the overall Security and Risk Management process, reviews presented Risk Assessment Reports and approves risk treatment plans or recommended controls.
Security Liaison	Security Liaisons are responsible for ensuring risk assessments are conducted, analyzing the risk and recommends controls, presenting risks for approval, documenting the process, and managing and facilitating the implementation of recommended controls.
System Owner / Administrator	System Owners/Administrators are responsible for participating in the identification and analysis process, participating in the risk identification and analysis process, and for the implementation of technical controls.
Functional Managers	Managers in the functional areas are responsible for participating in the risk identification and analysis process, and for the implementation of administrative controls.

SR-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 addresses the procedures and standards set forth by the State to implement the family of Supply Chain Risk Management security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the Supply Chain Risk Management security principles established in NIST SP 800-53, “Supply Chain Risk Management” control guidelines as the official policy for this security domain. The “SR” designator identified in each control represents the NIST-specified identifier for the Supply Chain Risk Management control family. The following subsections in this document outline the Supply Chain Risk Management requirements that each agency shall implement and maintain to manage risks that touch sourcing, vendor management, and supply chain quality across State agencies.

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.

SR -2 – Supply Chain Risk Management Plan

The following shall be implemented:

a. Develop a plan for managing supply chain risks associated with acquisition, delivery, integration, operations and maintenance, and disposal of the information systems and services:

DocuSign Envelope ID: 512C65D9-33EA-4DF8-AC77-1801BE7BE275

i The Supply Chain Risk Management (SCRM) plan should provide the basis for determining whether a technology, service or information system is fit for purpose and as such the controls need to be tailored accordingly.

ii The SCRM plan shall include the following:

1. an expression of the supply chain risk tolerance for the agency;
2. acceptable supply chain risk mitigation strategies or controls;
3. a process for consistently evaluating and monitoring supply chain risk;
4. approaches for implementing and communicating the plan;
5. a description of and justification for supply chain risk mitigation measures taken; and associated roles and responsibilities.

b. Review and update the supply chain risk management plan on an annual basis or as required, to address threat, organizational or environmental changes.

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2 (1) – Supply Chain Risk Management Plan | Establish SCRM Team

The following shall be implemented:

a. Establish a supply chain risk management team that consists of the agency-defined roles and is responsible for identifying, assessing, and managing risks while using coordinated efforts.

b. The SCRM team shall consist of personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executives, information technology, contracting, information security, privacy, mission, or business, legal, supply chain and logistics and acquisition.

c. The SCRM team shall be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

SR-3 – Supply Chain Controls and Processes

The following shall be implemented:

a. Establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems in coordination with the identified supply chain personnel.

i Supply chain elements include organizations, entities, or tools employed for the acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components.

DocuSign Envelope ID: 512C65D9-33EA-4DF8-AC77-1801BE7BE275

ii Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

b. Employ the following controls to protect against supply chain risks to information assets, systems, system components, or system services and to limit the harm or consequences from supply chain-related events (examples):

i Control Assessments (CA-2)
ii External System Services (SA-9)
iii Acquisition Process (SA-4)
iv Controlled Maintenance (MA-2)
v Component Authenticity (SR-11)
vi Component Disposal (SR-12)

c. Document the selected and implemented supply chain processes and controls in an agency-defined document such as a SCRM plan.

SR-5 – Acquisition Strategies, Tools, and Methods

Acquisition strategies, contract tools, and procurement methods shall be employed to protect against, identify, and mitigate supply chain risks. Examples are as follows:

a. Including incentive programs to system integrators, suppliers, or external services providers to ensure that they provide verification of integrity as well as traceability.

b. Requiring tamper-evident packaging.

c. Using trusted or controlled distribution.

SR-6 – Supplier Assessments and Reviews

Supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide shall be assessed and reviewed annually.
An assessment and review of supplier risk should include security and supply chain risk management processes, foreign ownership, and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

The reviews shall consider documented processes, documented controls, and publicly available information related to the supplier or contractor.

DocuSign Envelope ID: 512C65D9-33EA-4DF8-AC77-1801BE7BE275

This control is optional for LOW risk information systems.

SR-8 – Notification Agreements

Agreements and procedures with entities involved in the supply chain shall be established for the notification of supply chain compromises including security incident and a privacy breach and the notification of assessment or audit results.

SR-10 – Inspection of Systems or Components

A process to inspect information systems annually or upon any indications of the tampering of information systems shall be implemented.

Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

SR-11 – Component Authenticity

The following shall be implemented:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to the agency-defined personnel.

Organizations should include in their anti-counterfeit policy and procedures, a means to help ensure that the components acquired and used are authentic and have not been subject to tampering.

SR -11 (1) – Component Authenticity | Anti-Counterfeit Training

The following agency-defined roles shall be trained to detect counterfeit system components (including hardware, software, and firmware).

a. Personnel conducting configuration management activities
b. System administrators
c. Database administrators
d. Network administrators
e. Procurement personnel

DocuSign Envelope ID: 512C65D9-33EA-4DF8-AC77-1801BE7BE275

SR-11 (2) – Component Authenticity | Configuration Control for Component Service and Repair

Configuration control shall be maintained over system components awaiting service or repair and serviced or repaired components awaiting return to service.
Organizations shall manage risks associated with component repair including the repair process and any replacements, updates, and revisions of hardware and software components within the supply chain infrastructure.

SR-12 – Component Disposal

Defined data, documentation, tools, or system components shall be disposed of without exposing sensitive or operational information, which may lead to a future supply chain compromise. Examples include the following:

a. Monitoring and documenting the chain of custody through the destruction process.

b. Training disposal service personnel to ensure accurate delivery of service against disposal policy and procedures.

c. Implementing assessment procedures for the verification of disposal processes with a frequency that fits agency needs.

d. Using Media Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

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.

Approved: DocuSigned by: James Weaver 372C8D237F5547A... 1/19/2022 | 11:34 AM EST

Secretary of Department of Information Technology (DIT)