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. 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Material Superseded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 are responsible for adhering to this policy and any local Security Planning requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the State Chief Risk Officer (SCRO) or other designated organizational officials at the senior leadership level are assigned the responsibility for the continued development, dissemination, implementation, operation and monitoring of the Information Security Plan.
Agency Security Liaison	The Agency Security Liaison is the designated person who has overall responsibility for ensuring the security controls are implemented for their information systems. This role may be assigned to individuals with other agency responsibilities.
Information System Owner	The information system owner is the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. Develops and maintains the system security plan in coordination with information owners, the system administrator, the information system security officer, and functional "end users."
Information Owner	The information owner is the individual with operational responsibility and authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Provides input to information system owners regarding security requirements and security controls for the information system(s) where the information resides. Decides who has access to the information system and with

	what types of privileges or access rights. Assists in the identification and assessment of the common security controls where the information resides.
User	The user is an approved State or agency employee, contractor, or visitor who is authorized to use the IT system to conduct the business of the State or of an agency.
Third Parties	Third party service providers must provide Information Security plans and capabilities that meet State requirements. Third parties are required to maintain and update their plans on an annual basis or when there is a change in business requirements. Information Security plans are subject to periodic review of incident response controls by the State.

PL-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 requirements set forth by the State to implement the family of Security Planning security controls at the organization, process and/or system level for all information assets / State data. This policy provides requirements for the security planning process which is required to assure that information systems are designed and configured using controls sufficient to safeguard the State's information systems.

The State of North Carolina (State) has adopted the Security Planning principles established in NIST SP 800-53, "Security Planning" control guidelines as the official policy for this security domain. The "PL" designator identified in each control represents the NIST-specified identifier for the Security Planning control family. The following subsections in this document outline the Security Planning requirements that each agency must implement and maintain 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.

This control is optional for LOW risk information systems.

PL-2 – System Security and Privacy Plans

System Security and Privacy Plans (SSPPs) are a means to document security and privacy requirements and associated controls implemented within a given system. SSPPs also describe, at a high level, how the controls and control enhancements meet those security and privacy requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Agency SSPPs must meet the following requirements:

a. Include all critical systems and be consistent with the agency's enterprise architecture.

b. Explicitly define the constituent system components, e.g., authorization boundary for the system. An authorization boundary contains all components of an information system that are authorized for operation by an agency CIO or delegate and excludes separately authorized systems, to which the information system is connected.

c. Describe the operational context of the information system in terms of mission and business processes.

d. Identify the individuals that fulfill system roles and responsibilities.

e. Identify the information types processed, stored, and transmitted by the system.

f. Describe any specific threats to the system that are of concern to the organization.

g. Provide the results of a privacy risk assessment for systems processing Restricted or Highly Restricted data.

h. Provide an overview of the privacy requirements for the system.

i. Identify any relevant control baselines or overlays.

j. Describe the controls in place or planned for meeting the privacy requirements.

k. Include risk determinations for security and privacy architecture and design decisions.

l. Include security and privacy-related activities affecting the system that require planning and coordination with agency-defined individuals or groups.

m. Provide the security categorization of the information system including supporting rationale.

n. Describe the operational environment for the information system.

o. Describe relationships with or connections to other information systems.

p. Provide an overview of the security requirements for the system.

q. Describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.

r. Review and approve the security and privacy plan by the authorized representative prior to plan implementation.

s. Distribute copies of the security and privacy plan; and communicate subsequent changes to appropriate agency personnel.

t. Review the security and privacy plan for the information system on an annual basis.

u. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

v. Explicitly define the information systems that receive, process, store, or transmit Restricted or Highly Restricted data.

w. The System Security and Privacy Plan Template may be found on the following site: https://it.nc.gov/forms

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

PL-4 – Rules of Behavior

All information system users shall be provided the rules that describe their responsibilities and expected behavior about information and information system usage, security, and privacy. Organizations shall receive documented acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. The rules of behavior for State government use are described in the Statewide Acceptable Use Policy (AUP).

The Statewide Acceptable Use Policy (AUP) may be found via the following link: https://it.nc.gov/resources/state-it-policies

a. The AUP must be distributed to and acknowledged in writing by all information system users.

b. Documented acknowledgement from users indicating that they have read, understand, and agree to abide by the AUP must be received before they receive access to the information system.

c. Users must be trained on the AUP before they receive access to the information system.

d. The AUP shall be reviewed and updated annually, at a minimum.

PL-4 (1) – Rules of Behavior – Social Media and External Site/ Application Usage Restrictions

The following explicit restrictions shall be included in the AUP:

a. Restricted and Highly Restricted data shall not be shared on any social media/networking sites.

b. Posting agency information on public websites is not allowed.

c. The use of agency-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications shall be prohibited.

PL-5 – Privacy Impact Assessment

Withdrawn: Incorporated into RA-3, Risk Assessment.

PL-6 – Security-Related Activity Planning

Withdrawn: Incorporated into PL-2 (3).

PL-7 – Security Concept of Operations (Optional Control)

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

PL-8 – Security and Privacy Architectures

The statewide technical architecture shall be utilized as a requirement for the project review process. This information is captured within the Statewide Architectural Framework, which can be found at https://it.nc.gov/services/it-architecture/statewide-architecture-framework. Information security and privacy architectures shall include the following:

a. Description of the requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of agency information.

b. Description of the requirements and approach to be taken for processing Restricted and Highly Restricted data to minimize privacy risk to individuals.

c. Description of how the information security and privacy architectures are integrated into and support the enterprise architecture.

d. Description of any information security and privacy assumptions about, and dependencies on, external systems and services.

e. An annual review and update of the information security and privacy architectures to reflect changes in the enterprise architecture.

f. Planned architecture changes shall be reflected in the Security and Privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-9 – Central Management (Optional Control)

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

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)