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. §147-33.110, 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. These standards apply to all executive branch agencies, their agents or designees subject to Article 3D of N.C.G.S. §147. 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.

The State of North Carolina (State) has adopted the Security Planning principles established in NIST SP 800-53 Rev 4 "Security Planning" control guidelines as the official policy for this security domain. The "PL" designator identified in each procedure 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 develop, or adhere to in order to be compliant with 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, 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 (Moderate Control)

The State's security policies set forth the basic information technology security requirements for state government. Standing alone, it provides each executive branch agency with a basic information security manual. Some agencies may need to supplement the manual with more detailed policies and standards that relate to their specific operations and any applicable statutory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), the Internal Revenue Code, and the Payment Card Industry Data Security Standard (PCI DSS). This policy shall be reviewed annually, at a minimum.

PL-2 - System Security Plan (Moderate Control)

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

a. Develop a security plan for all critical systems that is consistent with the agency's enterprise architecture.

b. Explicitly define the 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 missions and business processes.

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

e. Describe the operational environment for the information system.

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

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

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

i. Review and approve the plan by the authorized representative prior to plan implementation.

j. Distribute copies of the security plan and communicate subsequent changes to the plan to appropriate agency personnel.

k. Review the security plan for the information system on an annual basis.

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

m. Explicitly define the information systems that receive, process, store, or transmit restricted or highly restricted data.

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

PL-2 (3) - System Security Plan – Coordinate with Other Entities (Moderate Control)

Agencies shall plan and coordinate security-related activities affecting an information system with any other agency entities (departments, divisions, management, etc.) before conducting such activities in order to reduce the impact on other agency entities.

Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by agencies to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.

a. Security-related activities affecting the information system must be planned and coordinated before such activities are conducted in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

b. System Owners shall identify and coordinate with the stakeholders and participants for each information system and security-related activity; these persons include, but are not limited to, the following:

   i. Business process owners

   ii. Users

   iii. Security personnel

   iv. Operations support personnel

   v. Appropriate personnel of connected systems

c. Security related activities that are planned or out of cycle must take into consideration other known events or resource cycles. If needed alternative times must be identified and reflected in appropriate budget documents.

PL-3 – System Security Plan Update (Moderate Control)

Withdrawn: Incorporated into PL-2.

PL-4 - Rules of Behavior

Agencies shall make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage. The State shall receive signed 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 are described in the Statewide Acceptable Use Policy (AUP).

The Statewide Acceptable Use Policy (AUP) can be accessed at the following: https://ncit.s3.amazonaws.com/s3fs-public/documents/files/Statewide-Acceptable-Use-Policy-3-16.pdf

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

b. Signed 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. Agencies shall include in the AUP, explicit restrictions on the use of social media/networking sites and posting agency information on public websites. Restricted and Highly Restricted data shall not be shared on any social media/networking sites.

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

PL-5 - Privacy Impact Assessment (Moderate Control)

Withdrawn: Incorporated into RA-3, Risk Assessment.

PL-6 – Security-Related Activity Planning (Moderate Control)

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 - Information Security Architecture

Agencies shall utilize the statewide technical architecture 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 architecture shall include the following:

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

b. Description of how the information security architecture is integrated into and supports the enterprise architecture.

c. Description of any information security assumptions about, and dependencies on, external services.

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

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: J.E. Bryant DBF6EB174A72411... 1/30/2018 | 8:25 PM EST

Secretary of Department of Information Technology (DIT)

Policy Approval and Review

Name	Reason	Date