	<h1>Personnel Security Policy</h1>	Document No. SCIO-SEC-311
Effective Date 01/29/2018	Review Date 01/18/2022	Version 3
		Page No. 1 of 6

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Material Superseded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 maintenance of information systems and supporting infrastructure are responsible for adhering to this policy and with any local personnel security 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 the personnel security protection program throughout the agencies.
Agency Security Liaison	The Agency Security liaison are responsible for ensuring that personnel security risks are managed in compliance with the State's requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate personnel security controls required for personnel security protection.
Human Resources	The Office of State Human Resources (OSHR) ensures that human resource policies and procedures are developed to satisfy the appropriate personnel security controls for the state.
Third Parties	Third party service providers are responsible for managing third party personnel in accordance with this policy.

	<h1>Personnel Security Policy</h1>	Document No. SCIO-SEC-311	
Effective Date 01/29/2018	Review Date 01/18/2022	Version 3	Page No. 2 of 6

PS-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 Personnel Security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the Personnel Security principles established in NIST SP 800-53, “Personnel Security” control guidelines as the official policy for this security domain. The “PS” designator identified in each control represents the NIST-specified identifier for the Personnel Security control family. The following subsections in this document outline the Personnel Security requirements that each agency must develop, or adhere to in order to protect the confidentiality, integrity and availability of agency mission critical information.


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.

PS-2 – Position Risk Designation

Information security responsibilities shall be assigned as an integral part of each organization’s information security program. Information security policy and job descriptions should provide general guidance on the various security roles and responsibilities within the organization.

- a. A risk designation shall be assigned to all system user positions and establish screening criteria for individuals filling those positions.
 - i. The following areas should be considered when they are defining security job responsibilities for system custodians and other managers with focused security positions (e.g., security analysts and business continuity planners):
 1. Identifying and clearly defining the various assets and security processes associated with each individual system for which the position holder will be held responsible.
 2. Clearly defining and documenting the agreed-upon authorization levels that the position holder will have to make enhancements, modify source code, promote updated code.
 - ii. Documenting for each asset shall include the following:
 1. Management’s assignment of system responsibility to a specific manager/custodian.
 2. Manager/custodian acceptance of responsibility for the system.

	<h1>Personnel Security Policy</h1>	Document No. SCIO-SEC-311
Effective Date 01/29/2018	Review Date 01/18/2022	Version 3
		Page No. 3 of 6

3. Detailed description of manager/custodian responsibilities.
 - b. Review and revise position risk designations annually and upon position vacancy or change in position description.
 - c. Application of this control is most often associated with positions requiring security clearances, or the completion of special training etc. that is required before access is granted to an individual.
 - d. Ensure that position risk designations are consistent with the requirements stated in the job classification policies published by the NC Office of State Human Resources (OSHR).

PS-3 – Personnel Screening


Personnel screening activities shall be defined to reflect applicable federal or state laws, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions, including the following:

- a. Conduct background investigations of individuals prior to authorizing access to agency information and information systems.
- b. Rescreen individuals as needed and in compliance with the State's personnel screening procedures. Recruitment procedures may be found in the policies published by the NC Office of State Human Resources (OSHR).
- c. Ensure that screening is consistent with the following:
 - i. OSHR policy, regulations, and guidance
 - ii. IRS 1075 guidance for systems containing federal tax information (FTI)
 - iii. The criteria established for the risk designation of the assigned position

PS-4 - Personnel Termination

The following shall be done upon termination of the individual's employment:

- a. Disable information system access immediately upon notification of termination.
- b. Disable user credentials immediately upon the account owner's termination from work for the State or when the account owner no longer needs access to the system or application due to a leave of absence or temporary reassignment.
- c. Conduct exit interviews to ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Exit interviews shall include, at a minimum, a discussion of nondisclosure agreements (NDAs) and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors.

	<h1>Personnel Security Policy</h1>	Document No. SCIO-SEC-311
Effective Date 01/29/2018	Review Date 01/18/2022	Version 3
		Page No. 4 of 6

- d. Retrieve all organizational information system-related property (e.g., keys, identification badges, State or agency owned issued mobile devices including laptops, tablets, cellular phones and hardware authentication tokens).
- e. Ensure that appropriate personnel retain access to data stored on a departing employee's information system.
- f. Notify the organization's help desk, security office, security guard, and the individual's manager immediately upon notification of termination of an individual or when there is the need to disable the information system accounts of individuals that are being terminated prior to the individuals being notified.

PS-5 - Personnel Transfer


Information systems facilities access authorizations shall be reviewed and confirmed when personnel are reassigned or transferred to other positions within the organization with the following required actions:

- a. Returning old and issuing new keys
- b. Issuing identification badges as required
- c. Closing old accounts and establishing new accounts
- d. Changing system access authorizations
- e. Providing access to data and accounts created or controlled by the employee at the old work location
- f. Notify agency personnel as required

PS-6 – Access Agreements

Appropriate signed access agreements shall be completed for individuals requiring access to information and information systems before authorizing access. The agreements shall be reviewed and updated annually, at a minimum.

- a. Access agreements may include the following:
 - i. Nondisclosure agreements (NDAs)
 - ii. Facility access agreements
 - iii. Acceptable use agreements
 - iv. Conflict-of-interest agreements
- b. Verify that individuals requiring access to information and information systems:


	<h1>Personnel Security Policy</h1>	Document No. SCIO-SEC-311
Effective Date 01/29/2018	Review Date 01/18/2022	Version 3
		Page No. 5 of 6

- i. Sign appropriate access agreements prior to being granted access; that include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized.
- ii. Re-sign access agreements to maintain access to information and information systems when access agreements have been updated or at least annually.
- c. All employee badge authorizations shall be reviewed semi-annually to verify the correct level of facility access for each employee. This review shall be conducted by the employee's manager and/or division director.
- d. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

PS-7 – External Personnel Security

Personnel security requirements shall be established, documented, and disseminated, including security roles and responsibilities for third-party providers. Third-party providers include vendors, suppliers, service bureaus, contractors, interns, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

- a. External providers shall comply with personnel security policies and procedures established by the organization. Third parties shall be fully accountable to the State for any actions taken while completing their assignments.
- b. Agency staff overseeing the work of external providers shall be responsible for communicating and enforcing applicable laws, as well as State and agency security policies, and procedures.
- c. Nondisclosure statements shall be signed by authorized representatives of the external provider before any information technology services are delivered.
- d. Agency operational and/or restricted information must not be released to external providers without properly executed contracts and confidentiality agreements. These contracts must specify conditions of use and security requirements and the access, roles, and responsibilities of the third party before access is granted.
- e. Access must be granted to external provider users only when required for performing work and with the full knowledge and prior approval of the information asset owner.
- f. All new connections between external provider and State agencies shall be documented in an agreement that includes information technology security requirements for the connections. The agreement shall be signed by an agency employee who is legally authorized to sign on behalf of the agency and by a representative from the external provider who is legally authorized to sign on behalf of the external provider. The signed document must be kept on file with the relevant group.

	<h1>Personnel Security Policy</h1>	Document No. SCIO-SEC-311
Effective Date 01/29/2018	Review Date 01/18/2022	Version 3 Page No. 6 of 6

- g. External providers shall notify the Agency Security Liaison or other designated agency personnel of any transfers or terminations of external provider personnel who possess organizational credentials or badges, or who have information system privileges as soon as transfers or terminations are known and a justification for the replacement request is submitted.
- h. Agencies shall define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred.
- i. Contracts with external providers providing offsite hosting or cloud services must require the external provider to provide the State with an annual independent risk assessment report to establish compliance with N.C.G.S. 143B-1378.
- j. Agencies shall monitor external provider compliance with personnel security requirements.

PS-8 – Personnel Sanctions

A formal sanctions process shall be employed for personnel failing to comply with established information security policies and procedures.

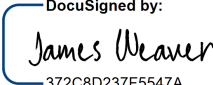
- a. Notify the OSHR immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction
- b. Ensure that the sanctions process is consistent with the employee disciplinary policy published by the NC Office of State Human Resources (OSHR).

PS-9 – Position Descriptions

Security and privacy roles and responsibilities shall be incorporated into organizational position descriptions.

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:  1/19/2022 | 11:34 AM EST
372C8D237E5547A

Secretary of Department of Information Technology (DIT)