	Security Awareness and Training Policy		**Document No.** SCIO-SEC-302
Effective Date 01/29/2018	**Review Date** 03/26/2025	**Version** 4	**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Material Superseded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 are accountable for the accuracy, integrity, and confidentiality of the information to which they have access. All covered personnel who utilize IT resources are responsible for adhering to this policy.

Role	Definition
Information Security Officer	The Agency Security Liaison, Information Security Officer (ISO), Chief Information Officer (CIO), 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 security awareness training program.
Agency Management	Managers must stay current in their training to oversee departmental and local information security. They must also stay current in their training to effectively develop, document, maintain, test, and oversee any required local information security policies, and training materials. This training must also cover local and departmental requirements. All levels of management must ensure employees, contractors, and vendors adhere to approved information security procedures by ensuring staff are informed about their

	security responsibilities and attain continued education relevant to information security and their position in the organization.
Covered Personnel	Covered personnel are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of compromise of information or information systems managed by the State.
Third Parties	Third party service providers must comply with State information security awareness and training requirements

AT-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 and Awareness Training controls at the organization, process and/or system level for all information assets / State data. This policy provides the security awareness and training requirements which are required to establish the necessary security best practices to secure State information assets.

The State of North Carolina (State) requires all users of systems managed by the State to be provided training on relevant cybersecurity and physical security threats and safeguards by their respective agencies. Each individual is required to complete introductory and annually recurring security awareness training to ensure that all employees, contractors and third parties are familiar with information security policies, as well as departmental and local information security responsibilities.

The State has adopted the Security Awareness and Training principles established in NIST SP 800-53, “Security Awareness and Training,” control guidelines, as the official policy for this security domain. The “AT” designator identified in each control represents the NIST-specified identifier for the Security Awareness and Training control family. The following subsections in this document outline the Security Awareness and Training 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.

The senior management of each agency shall lead by example by ensuring that information security is given a high priority. Agency senior management shall ensure that information security communications are given priority by staff and shall support information security awareness programs. All agencies shall provide new employees and contractors with mandatory information security training as part of job orientation. The agency shall provide regular and relevant information security awareness communications to all staff by various means, which may include the following:

a. Electronic updates, briefings, pamphlets, and newsletters.

b. Self-based information security awareness training to enhance awareness and educate staff on information technology security threats and the appropriate safeguards.

c. An employee handbook or summary of information security policies, which shall be formally delivered to and acknowledged by employees before they access agency resources.

All users of new systems shall receive training to ensure that their use of the systems is effective and does not compromise information security. Agencies shall train users on how new systems will integrate into their current responsibilities. Agencies shall notify staff of all existing and any new policies that apply to new systems.

AT-2 - Security Training and Awareness

Management must provide any required organizational cybersecurity and privacy training in addition to State required training and track the completion of all required training in a training completion log or system. Information relevant to effective cybersecurity and privacy practices shall be provided to staff members and system users (including managers, senior executives, and contractors) in a timely manner. On an annual basis, management shall receive input from cybersecurity and privacy staff on the effectiveness of cybersecurity and privacy measures and recommended improvements. Training requirements include the following:

a. A handbook or summary of cybersecurity and privacy policies, which shall be formally delivered to and signed by covered persons before beginning work.

b. Formal cybersecurity and privacy training appropriate for work responsibilities shall be provided on a regular basis and whenever their work responsibilities change.

c. Managers must delay covered personnel access to Restricted or Highly Restricted data until initial training is complete. Training to users shall also be provided when required by system changes or following agency-defined events that require such training.

d. When staff members change jobs, their information security and privacy needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority.

e. Agencies shall employ the following awareness techniques to increase the security and privacy awareness of system users:

   i Requiring interactive training modules

   ii Distributing cybersecurity newsletters and other publications

   iii Providing/promoting cybersecurity webinars

   iv Conducting phishing simulations

   v Displaying cybersecurity themed posters in common areas

   vi Displaying cybersecurity themed messages on device screensavers

   vii Distributing email advisories or notices

   viii Conducting awareness events

f. Lessons learned from internal or external security or privacy incidents should be incorporated into training and awareness techniques.

g. Training and awareness content shall be updated annually and following agency-defined events that require it to be updated.

h. All external personnel, e.g., contractors and other third parties, shall have provisions in their contracts with State agencies that set forth the requirement that they must comply with all agency information security policies, including any required awareness and training. See Personnel Security Policy PS-7 External Personnel Security for additional requirements for external personnel.

i. Training on social engineering and how to detect it and respond to it.

j. Training on the acceptable use of State resources.

k. Annually recurring cybersecurity and privacy awareness training in support of the program objectives must be completed by each covered person (which includes all employees, contractors, consultants, and vendors with access to State information assets) that is appropriate for work responsibilities. The cybersecurity and privacy awareness training is in addition to any other agency specific or regulatory training that may also be required.

l. Management must revoke logical access to systems and services if an employee fails to complete required annually training. Failure to complete required training within the renewal date shall result in either disciplinary action or a loss of access to systems until such time as the training has been completed.

m. Persons on extended medical leave are exempted from this requirement until such time that they return to the workplace.

n. Managers must ensure that covered persons remain in compliance with required training.

o. Long term contractors and other third parties with contracts ending within 30 days of a training deadline are exempted from completing any currently assigned training. If a third-party individual's contract is extended, however, the individual is required to complete their assigned training.

AT-2 (2) - Security Training and Awareness | Insider Threat

An insider threat is an entity with authorized access that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. Insider threat training shall be provided that includes how to communicate employee and management concerns and the prevention, detection, and response regarding potential indicators of insider threats through appropriate agency's channels in accordance with established organizational policies and procedures.

Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices.

AT-2 (3) – Security Training and Awareness | Social Engineering and Mining

Training on recognizing and reporting potential and actual instances of social engineering and social mining shall be provided. Some examples of this training include the following:

a. Distributing examples of phishing email

b. Conducting phishing simulations

c. Posting successful findings from reputable news sources

AT-3 - Role Based Training

The extent of security and privacy related training shall reflect the person's individual responsibility for using, configuring, and/or maintaining information systems. It should also reflect the privacy requirements of the agency or organization. Training in critical areas of cybersecurity, privacy, including vendor-specific recommended safeguards, shall be provided to users and technical staff.

a. Role based security and privacy-related training shall be provided before authorizing a person's access to a system and before they are allowed to perform their assigned duties, when required by system changes.

b. Role based training content shall be updated annually and following agency-defined events that require it to be updated.

c. Lessons learned from internal or external security or privacy incidents should be incorporated into role-based training.

d. Training in cybersecurity threats and safeguards, with the technical details to reflect the staff's individual responsibility for configuring and maintaining information security is required.

e. Annual re-occurring training shall be provided thereafter.

f. Technical staff responsible for information system security will receive training in the following areas:

   i. Server and PC security engagement.

   ii. Packet-filtering techniques implemented on routers, firewalls, etc.

   iii. Intrusion detection and prevention.

   iv. Software configuration, change and patch management.

   v. Virus prevention/protection procedures.

   vi. Business continuity practices and procedures.

g. Additional education for information security and privacy professionals and jobs requiring expertise in security and privacy will be provided as needed through formal external courses and certification programs.

AT-4 - Training Records

Agencies and organizations shall document and monitor individual information system security and privacy training activities, including basic security awareness training and specific role-based information system security and privacy training. Individual training records shall be retained for a period of five years.

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.