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. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. 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.

Responsibilities

All covered personnel are accountable for the accuracy, integrity, and confidentiality of the information to which they have access. All covered personnel that 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, 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

Policy

The State of North Carolina (State) requires that all users of systems managed by the State must 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.

This policy documents the security awareness and training requirements for the State and its Agencies to establish the necessary security best practices required to secure the State's information assets.

The State has adopted the Security Awareness and Training principles established in NIST SP 800-53 "Security Awareness and Education," control guidelines, as the official policy for this security domain. The "AT" designator identified in each procedure 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 develop, or adhere to in order to be compliant with this policy. This policy shall be reviewed annually, at a minimum.

AT-1 - Security Awareness Program Delivery

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 Awareness Training

Agency management must provide any required local information security training in addition to State required training and track the completion of all required training in a training completion log or system. Agencies shall provide information relevant to effective information security practices to staff members in a timely manner. On a periodic basis, agency management shall receive input from information security staff on the effectiveness of information security measures and recommended improvements. Training requirements include the following:

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

b. Formal information technology security training appropriate for work responsibilities, 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.

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

e. All 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.

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

g. Training on the acceptable use of State resources.

h. Annually recurring information security awareness training in support of information security awareness 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.

i. 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.

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

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

l. Long term contractors and other third parties with contracts ending within 30 days of an annual training deadline are exempted from completing annual training.

AT-2 (2) - Security Awareness Training – Insider Threat (Moderate Control)

Insider threat training shall include 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-3 - Role Based Security Awareness Training

The extent of security related training shall reflect the person's individual responsibility for using, configuring, and/or maintaining information systems. Agencies shall provide training to users and technical staff in critical areas of cybersecurity, including vendor-specific recommended safeguards.

a. Role based security-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. 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.

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

d. 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.

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

AT-4 - Security Training Records

Agencies shall document and monitor individual information system security training activities, including basic security awareness training and specific information system security 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.

Approved: DocuSigned by: DBF6EB174A72411... 1/30/2018 | 8:25 PM EST

Secretary of Department of Information Technology (DIT)

Policy Approval and Review

Name	Reason	Date