# North Carolina Department of Information Technology

# Statewide Information Security Manual

March 2025

# Statewide Information Security Manual

## INTRODUCTION

### PURPOSE

The purpose of this policy is to establish a statewide security policy for North Carolina State agencies and the State network. This policy also establishes principles to ensure a secure network infrastructure that integrates confidentiality, availability, and integrity into the infrastructure design, implementation, and maintenance, to do the following:

a. Protect the State's infrastructure and the citizen's data, whether hosted by external entities or within State data centers, from both internal and external threats.

b. Provide a consistent and repeatable framework for which IT assets can be securely connected to the State network.

c. Support the State's initiative to establish standards to manage technology, risks and increase consistency and accessibility.

### OWNER

State Chief Information Security Officer

### SCOPE

The Statewide Information Security Manual is the foundation for information technology security in North Carolina. It sets 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. These security policies are consistent with applicable laws, executive orders, directives, regulations, and other policies, standards, and guidelines.

## POLICY

### SECTION 1. ADOPTION OF NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RISK MANAGEMENT FRAMEWORK SPECIAL PUBLICATION (SP) 800-37

The State has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 – *Guide for Applying Risk Management Framework (RMF) for Federal Information Systems,* as the standard for managing information security risk in State IT resources. The RMF provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The NIST RMF utilizes NIST SP 800-53 as the foundation for identifying and implementing security controls. NIST 800-53

organizes these security controls into eighteen (18) Control Families. Each policy document and control family identified in the Statewide Information Security Manual is based on the NIST SP 800-53, Security and Privacy Controls. The State has modified certain controls from the original NIST 800-53 requirements where they were deemed necessary.

Table 1 below identifies the control family names which will be utilized within the State security policies.

**TABLE 1: SECURITY CONTROL FAMILY NAMES**

| ID | FAMILY | ID | FAMILY |
|---|---|---|---|
| AC | Access Control | MP | Media Protection |
| AT | Awareness and Training | PE | Physical and Environmental Protection |
| AU | Audit and Accountability | PL | Security Planning |
| CA | Assessment, Authorization, and Monitoring | PS | Personnel Security |
| CM | Configuration Management | RA | Risk Assessment |
| CP | Contingency Planning | SA | System and Services Acquisition |
| IA | Identification and Authentication | SC | System and Communications Protection |
| IR | Incident Response | SI | System and Information Integrity |
| MA | Maintenance | SR | Supply Chain Risk Management |

## SECURITY CATEGORIZATION

There are two levels of security categorization to be used within the State: ***Low*** and ***Moderate***. Security controls must be selected based on the data classification and security categorization of the information system and/or requirements for the specific operating environment.

> **Low Systems**: Systems that contain only data that is public by law or directly available to the public via such mechanisms as the Internet. In addition, desktops, laptops and supporting systems used by agencies are Low Risk unless they store, process, transfer or communicate Restricted or Highly Restricted data.
>
> **Moderate Systems**: Systems that store, process, transfer or communicate Restricted or Highly Restricted data or have a direct dependency on a Moderate system. Any system that stores, processes, or transfers or communicates PII or other sensitive data types is classified as a Moderate system, at a minimum.

**Agencies may tailor the baseline controls, as needed to enhance the security posture, based on their unique organizational needs**. An example of such enhancement may occur due to additional requirements mandated by Federal agencies such as Internal Revenue Service (IRS) and other. All agencies are required to implement and comply with the baseline controls within the Statewide Information Security Manual, unless otherwise prescribed by Federal or State statute. Any deviations to required security controls must be submitted for approval through the DIT Exception Process.

NIST SP 800-53 controls defines three types of controls:

- ***Common Controls****:* Those security controls that are Enterprise wide, e.g., State policies, Security devices provided by DIT, Enterprise email, etc. Agencies may inherit these controls as the system is managed outside of their authority. It is important to note that for a system to be considered **Inherited,** it must meet, at a minimum, the following criteria:
    - The system is managed by DIT, Cloud or other organizations outside the authority and security boundary of the agency,
    - The State Chief Risk Officer has designated the control as inheritable.

- ***System-Specific Controls****:* Those controls that provide security and other services for a particular information system only.
- ***Hybrid Controls****:* Those controls which are shared between Enterprise, i.e., DIT, Cloud and/or Agency managed.

Agencies must evaluate each system and identify those that fall within the above listed control types. This step is crucial in facilitating and understanding roles and responsibilities as it pertains to audits and assessments. The following Table 2 - *Security Control Baseline* identifies those controls that will be implemented if a system is categorized as Low or Moderate. The table is based on NIST 800-53 Rev 5 and has been modified to meet State of North Carolina use.

**Note:** Controls which have brackets, i.e., (X), are "control enhancements" above the base requirement. Controls listed as "Optional" may be utilized to enhance the security posture of the information system and are NOT considered mandatory. Agencies should understand that with the implementation of optional controls may require additional funding. The description of these controls may be found at the following link:

https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/families?version=5.1

**TABLE 2: SECURITY CONTROL BASELINES**

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| **Access Control** | | | |
| AC-1 | Access Control Policy and Procedures | AC-1 | AC-1 |
| AC-2 | Account Management | AC-2 | AC-2 (1) (2) (3) (4) (5) (13) |
| AC-3 | Access Enforcement | AC-3 | AC-3 |
| AC-4 | Information Flow Enforcement | AC-4 | AC-4 |
| AC-5 | Separation of Duties | AC-5 | AC-5 |
| AC-6 | Least Privilege | AC-6 | AC-6 (1) (2) (5) (7) (9) (10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | AC-7 |
| AC-8 | System Use Notification | AC-8 | AC-8 |
| AC-9 | Previous Logon (Access) Notification | Optional | Optional |
| AC-10 | Concurrent Session Control | Optional | Optional |
| AC-11 | Device Lock | AC-11 | AC-11 (1) |
| AC-12 | Session Termination | AC-12 | AC-12 |
| AC-14 | Permitted Actions without Identification or Authentication | AC-14 | AC-14 |
| AC-16 | Security Attributes | Optional | Optional |
| AC-17 | Remote Access | AC-17 | AC-17 (1) (2) (3) (4) |
| AC-18 | Wireless Access | AC-18 | AC-18 (1) (3) |
| AC-19 | Access Control for Mobile Devices | AC-19 | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | AC-20 (1) (2) |
| AC-21 | Information Sharing | Optional | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | AC-22 |
| AC-23 | Data Mining Protection | Optional | Optional |
| AC-24 | Access Control Decisions | Optional | Optional |
| AC-25 | Reference Monitor | Optional | Optional |

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| **Awareness and Training** | | | |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | AT-1 |
| AT-2 | Security Training and Awareness | AT-2 | AT-2 (2) (3) |
| AT-3 | Role-Based Training | AT-3 | AT-3 |
| AT-4 | Training Records | AT-4 | AT-4 |
| **Audit and Accountability** | | | |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | AU-1 |
| AU-2 | Event Logging | AU-2 | AU-2 |
| AU-3 | Content of Audit Records | AU-3 | AU-3 (1) |
| AU-4 | Audit Storage Capacity | AU-4 | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | AU-5 |
| AU-6 | Audit Review, Analysis, and Reporting | AU-6 | AU-6 (1) (3) |
| AU-7 | Audit Reduction and Report Generation | Optional | AU-7 |
| AU-8 | Time Stamps | AU-8 | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | AU-9 (4) |
| AU-10 | Non-repudiation | Optional | Optional |
| AU-11 | Audit Record Retention | AU-11 | AU-11 |
| AU-12 | Audit Record Generation | AU-12 | AU-12 |
| AU-13 | Monitoring for Information Disclosure | Optional | Optional |
| AU-14 | Session Audit | Optional | Optional |
| AU-15 | Alternate Audit Capability | Optional | Optional |
| AU-16 | Cross-Organizational Audit Logging | Optional | Optional |
| **Assessment, Authorization and Monitoring** | | | |
| CA-1 | Security Assessment, Authorization and Monitoring Policy and Procedures | CA-1 | CA-1 |
| CA-2 | Control Assessments | CA-2 | CA-2 (1) |
| CA-3 | Information Exchange | CA-3 | CA-3 (5) |
| CA-4 | Security Certification | Incorporated into CA-2. | Incorporated into CA-2. |
| CA-5 | Plan of Action and Milestones/ Corrective Action Plan | CA-5 | CA-5 |
| CA-6 | Authorization | CA-6 | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 (4) | CA-7 (1) (4) |
| CA-8 | Penetration Testing | Optional | CA-8 |
| CA-9 | Internal System Connections | CA-9 | CA-9 |
| **Configuration Management** | | | |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (2) (3) (7) |
| CM-3 | Configuration Change Control | CM-3 | CM-3 (4) |
| CM-4 | Impact Analysis | CM-4 | CM-4 (2) |
| CM-5 | Access Restrictions for Change | CM-5 | CM-5 |
| CM-6 | Configuration Settings | CM-6 | CM-6 |

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| CM-7 | Least Functionality | CM-7 (1) | CM-7 (1) (2) (5) |
| CM-8 | System Component Inventory | CM-8 (1) | CM-8 (1) (3) |
| CM-9 | Configuration Management Plan | CM-9 | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 |
| CM-11 | User-Installed Software | CM-11 | CM-11 |
| CM-12 | Information Location | CM-12 | CM-12 (1) |
| **Contingency Planning** | | | |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | CP-2 |
| CP-3 | Contingency Training | CP-3 | CP-3 |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 |
| CP-5 | Contingency Plan Update | Incorporated into CP-2 | Incorporated into CP-2 |
| CP-6 | Alternate Storage Site | Optional | CP-6 |
| CP-7 | Alternate Processing Site | Optional | CP-7 |
| CP-8 | Telecommunications Services | Optional | CP-8 |
| CP-9 | System Backup | CP-9 | CP-9 (1) (8) |
| CP-10 | System Recovery and Reconstitution | CP-10 | CP-10 |
| CP-11 | Alternate Communications Protocols | Optional | Optional |
| CP-12 | Safe Mode | Optional | Optional |
| CP-13 | Alternative Security Mechanisms | Optional | Optional |
| **Identification and Authentication** | | | |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (8) | IA-2 (1) (2) (8) (12) |
| IA-3 | Device Identification and Authentication | IA-3 | IA-3 |
| IA-4 | Identifier Management | IA-4 | IA-4 |
| IA-5 | Authenticator Management | IA-5 (1) | IA-5 (1) (6) |
| IA-6 | Authenticator Feedback | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 | IA-8 |
| IA-9 | Service Identification and Authentication | Optional | Optional |
| IA-10 | Adaptive Authentication | Optional | Optional |
| IA-11 | Re-authentication | IA-11 | IA-11 |
| IA-12 | Identity Proofing | Optional | IA-12 (2) (3) (5) |
| **Incident Response** | | | |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | IR-2 |
| IR-3 | Incident Response Testing | Optional | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) |
| IR-5 | Incident Monitoring | IR-5 | IR-5 |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) (3) |

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1) |
| IR-8 | Incident Response Plan | IR-8 | IR-8 |
| IR-9 | Information Spillage Response | Optional | Optional |
| IR-10 | Integrated Information Security Analysis Team | Optional | Optional |
| **Maintenance** | | | |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | MA-2 |
| MA-3 | Maintenance Tools | Optional | MA-3 (1) (2) (3) |
| MA-4 | Nonlocal Maintenance | MA-4 | MA-4 |
| MA-5 | Maintenance Personnel | MA-5 | MA-5 |
| MA-6 | Timely Maintenance | Optional | MA-6 |
| **Media Protection** | | | |
| MP-1 | Media Protection Policy and Procedures | MP-1 | MP-1 |
| MP-2 | Media Access | MP-2 | MP-2 |
| MP-3 | Media Marking | Optional | MP-3 |
| MP-4 | Media Storage | Optional | MP-4 |
| MP-5 | Media Transport | Optional | MP-5 |
| MP-6 | Media Sanitization | MP-6 | MP-6 |
| MP-7 | Media Use | MP-7 | MP-7 (1) |
| MP-8 | Media Downgrading | Optional | Optional |
| **Physical and Environmental Protection** | | | |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | PE-2 |
| PE-3 | Physical Access Control | PE-3 | PE-3 |
| PE-4 | Access Control for Transmission | PE-4 | PE-4 |
| PE-5 | Access Control for Output Devices | Optional | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | PE-6 (1) |
| PE-8 | Visitor Access Records | PE-8 | PE-8 |
| PE-9 | Power Equipment and Cabling | Optional | PE-9 |
| PE-10 | Emergency Shutoff | Optional | PE-10 |
| PE-11 | Emergency Power | Optional | PE-11 |
| PE-12 | Emergency Lighting | PE-12 | PE-12 |
| PE-13 | Fire Protection | PE-13 | PE-13 (1) |
| PE-14 | Environmental Controls | PE-14 | PE-14 |
| PE-15 | Water Damage Protection | PE-15 | PE-15 |
| PE-16 | Delivery and Removal | PE-16 | PE-16 |
| PE-17 | Alternate Work Site | Optional | PE-17 |
| PE-18 | Location of System Components | Optional | PE-18 |
| PE-19 | Information Leakage | Optional | Optional |
| PE-20 | Asset Monitoring and Tracking | Optional | Optional |
| **Security Planning** | | | |

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| PL-1 | Security Planning Policy and Procedures | Optional | PL-1 |
| PL-2 | System Security and Privacy Plans | Optional | PL-2 |
| PL-4 | Rules of Behavior | PL-4 (1) | PL-4 (1) |
| PL-5 | Privacy Impact Assessment | Optional | Incorporated in RA-3 |
| PL-7 | Security Concept of Operations | Optional | Optional |
| PL-8 | Information Security Architecture | PL-8 | PL-8 |
| PL-9 | Central Management | Optional | Optional |
| **Personnel Security** | | | |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | PS-2 |
| PS-3 | Personnel Screening | PS-3 | PS-3 |
| PS-4 | Personnel Termination | PS-4 | PS-4 |
| PS-5 | Personnel Transfer | PS-5 | PS-5 |
| PS-6 | Access Agreements | PS-6 | PS-6 |
| PS-7 | External Personnel Security | PS-7 | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | PS-8 |
| PS-9 | Position Descriptions | PS-9 | PS-9 |
| **Risk Assessment** | | | |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | RA-1 |
| RA-2 | Security Categorization | RA-2 | RA-2 |
| RA-3 | Risk Assessment | RA-3 | RA-3 |
| RA-4 | Risk Assessment Update | Incorporated into RA-3 | Incorporated into RA-3 |
| RA-5 | Vulnerability Monitoring and Scanning | RA-5 | RA-5 (1) (2) (5) |
| **System and Services Acquisition** | | | |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | SA-4 (1) (2) (9) (10) |
| SA-5 | System Documentation | SA-5 | SA-5 |
| SA-8 | Security and Privacy Engineering Principles | Optional | SA-8 |
| SA-9 | External System Services | SA-9 | SA-9 (2) |
| SA-10 | Developer Configuration Management | Optional | SA-10 |
| SA-11 | Developer Testing and Evaluation | Optional | SA-11 |
| SA-12 | Supply Chain Protection | Optional | Optional |
| SA-13 | Trustworthiness | Optional | Optional |
| SA-14 | Criticality Analysis | Optional | Optional |
| SA-15 | Development Process, Standards, and Tools | Optional | Optional |
| SA-16 | Developer-Provided Training | Optional | Optional |
| SA-17 | Developer Security Architecture and Design | Optional | Optional |
| SA-18 | Tamper Resistance and Detection | Optional | Optional |
| SA-19 | Component Authenticity | Optional | Optional |

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| SA-20 | Customized Development of Critical Components | Optional | Optional |
| SA-21 | Developer Screening | Optional | Optional |
| SA-22 | Unsupported System Components | SA-22 | SA-22 |
| **System and Communications Protection** | | | |
| SC-1 | System and Communications Protection Policy and Procedures | SC-1 | SC-1 |
| SC-2 | Separation of System and User Functionality | SC-2 | SC-2 |
| SC-3 | Security Function Isolation | Optional | Optional |
| SC-4 | Information in Shared System Resources | Optional | SC-4 |
| SC-5 | Denial of Service Protection | SC-5 | SC-5 |
| SC-6 | Resource Availability | Optional | Optional |
| SC-7 | Boundary Protection | SC-7 | SC-7 (4) (5) (7) (8) |
| SC-8 | Transmission Confidentiality and Integrity | SC-8 | SC-8 (1) |
| SC-10 | Network Disconnect | SC-10 | SC-10 |
| SC-11 | Trusted Path | Optional | Optional |
| SC-12 | Cryptographic Key Establishment and Management | SC-12 | SC-12 |
| SC-13 | Cryptographic Protection | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices and Applications | SC-15 | SC-15 |
| SC-16 | Transmission of Security and Privacy Attributes | Optional | Optional |
| SC-17 | Public Key Infrastructure Certificates | SC-17 | SC-17 |
| SC-18 | Mobile Code | SC-18 | SC-18 |
| SC-19 | Voice Over Internet Protocol | Optional | SC-19 |
| SC-20 | Secure Name/Address Resolution Service (Authoritative Source) | SC-20 | SC-20 |
| SC-21 | Secure Name/Address Resolution Service (Recursive or Caching Resolver) | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name/Address Resolution Service | SC-22 | SC-22 |
| SC-23 | Session Authenticity | SC-23 | SC-23 |
| SC-24 | Fail in Known State | Optional | Optional |
| SC-25 | Thin Nodes | Optional | Optional |
| SC-26 | Decoys | Optional | Optional |
| SC-27 | Platform-Independent Applications | Optional | Optional |
| SC-28 | Protection of Information at Rest | Optional | SC-28 (1) |
| SC-29 | Heterogeneity | Optional | Optional |
| SC-30 | Concealment and Misdirection | Optional | Optional |
| SC-31 | Covert Channel Analysis | Optional | Optional |
| SC-32 | System Partitioning | Optional | Optional |
| SC-34 | Non-Modifiable Executable Programs | Optional | Optional |
| SC-35 | External Malicious Code Identification | Optional | Optional |
| SC-36 | Distributed Processing and Storage | Optional | Optional |
| SC-37 | Out-of-Band Channels | Optional | Optional |

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | |
|---|---|---|---|
| | | LOW | MOD |
| SC-38 | Operations Security | Optional | Optional |
| SC-39 | Process Isolation | Optional | Optional |
| SC-40 | Wireless Link Protection | SC-40 | SC-40 |
| SC-41 | Port and I/O Device Access | Optional | Optional |
| SC-42 | Sensor Capability and Data | Optional | Optional |
| SC-43 | Usage Restrictions | SC-43 | SC-43 |
| SC-44 | Detonation Chambers | Optional | SC-44 |
| **System and Information Integrity** | | | |
| SI-1 | System and Information Integrity Policy and Procedures | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | SI-2 | SI-2 (2) |
| SI-3 | Malicious Code Protection | SI-3 | SI-3 |
| SI-4 | System Monitoring | SI-4 | SI-4 (2) (4) (5) |
| SI-5 | Security Alerts, Advisories, and Directives | SI-5 | SI-5 |
| SI-6 | Security and Privacy Function Verification | Optional | Optional |
| SI-7 | Software, Firmware, and Information Integrity | Optional | SI-7 (1) (7) |
| SI-8 | Spam Protection | Optional | SI-8 (1) (2) |
| SI-10 | Information Input Validation | Optional | SI-10 |
| SI-11 | Error Handling | Optional | SI-11 |
| SI-12 | Information Management and Retention | SI-12 | SI-12 |
| SI-13 | Predictable Failure Prevention | Optional | Optional |
| SI-14 | Non-Persistence | Optional | Optional |
| SI-15 | Information Output Filtering | Optional | Optional |
| SI-16 | Memory Protection | Optional | SI-16 |
| SI-17 | Fail-Safe Procedures | Optional | Optional |
| **Supply Chain Risk Management** | | | |
| SR-1 | Supply Chain Risk Management Policy and Procedures | SR-1 | SR-1 |
| SR-2 | Supply Chain Risk Management Plan | SR-2 (1) | SR-2 (1) |
| SR-3 | Supply Chain Controls and Processes | SR-3 | SR-3 |
| SR-4 | Provenance | Optional | Optional |
| SR-5 | Acquisition Strategies, Tools, and Methods | SR-5 | SR-5 |
| SR-6 | Supplier Assessments and Reviews | Optional | SR-6 |
| SR-7 | Supply Chain Operations Security | Optional | Optional |
| SR-8 | Notification Agreements | SR-8 | SR-8 |
| SR-9 | Tamper Resistance and Detection | Optional | Optional |
| SR-10 | Inspection of Systems or Components | SR-10 | SR-10 |
| SR-11 | Component Authenticity | SR-11 (1) (2) | SR-11 (1) (2) |
| SR-12 | Component Disposal | SR-12 | SR-12 |

## SECTION 2. IMPLEMENTATION AND MANAGEMENT

This Manual is the foundation for information technology security in state government and is required for all executive branch agencies to follow in order to comply with statewide information security standards. To be successful, Agency leadership must continue to emphasize the importance of information security throughout their organizations and at their discretion, implement additional supplementary controls as deemed necessary. When considering the supplementary controls not included in the State's policies, agencies should refer to NIST SP 800-53 Rev 5 and industry security practices related to information technology implementation. Agencies are also required to ensure ongoing compliance by implementing continuous monitoring activities.

## SECTION 3 – INFORMATION PROTECTION

Agencies must implement appropriate safeguards as defined in the supporting policy documents (such as identification and authentication, encryption, data filtering, tagging, Multi-factor authentication or segregation) to ensure Restricted and Highly Restricted information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Payment Card Industry (PCI) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements.

Agencies must ensure an appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

## SECTION 4 – CONTINUOUS MONITORING

Continuous monitoring, automatic alerting, and auditing with corresponding tracking capabilities and reporting are required for devices connected to the State infrastructure or supporting State business (e.g., cloud services). Agencies must also have procedures in place to ensure robust incident response to unauthorized accesses and activities. The State CIO has the authority to require the installation of monitoring or auditing agents on devices connected to the network.

## SECTION 5 – SECURITY ARCHITECTURE

Agencies must implement appropriate information safeguards (such as encryption, data filtering, tagging, or segregation) to ensure highly restricted information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Payment Card Industry (PCI) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements.

Agencies must ensure an appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

## SECTION 4 – REFERENCES

The following policies in the Statewide Information Security Manual provide additional details for the implementation of State information technology resources.

- SCIO-SEC-301: Access Control Policy (AC)
- SCIO-SEC-302: Awareness and Training Policy (AT)
- SCIO-SEC-303: Audit and Accountability Policy (AU)
- SCIO-SEC-304: Assessment, Authorization, and Monitoring Policy (CA)

- SCIO-SEC-305: Configuration Management Policy (CM)
- SCIO-SEC-306: Contingency Planning Policy (CP)
- SCIO-SEC-307: Identification and Authentication Policy (IA)
- SCIO-SEC-308: Incident Response Policy (IR)
- SCIO-SEC-309: Maintenance Policy (MA)
- SCIO-SEC-310: Media Protection Policy (MP)
- SCIO-SEC-311: Personnel Security Policy (PS)
- SCIO-SEC-312: Security Planning Policy (PL)
- SCIO-SEC-313: Physical and Environmental Protection Policy (PE)
- SCIO-SEC-314: Risk Assessment Policy (RA)
- SCIO-SEC-315: System and Services Acquisition Policy (SA)
- SCIO-SEC-316: System and Communications Protection Policy (SC)
- SCIO-SEC-317: System and Information Integrity Policy (SI)
- SCIO-SEC-318: Supply Chain Risk Management Policy (SR)

**Approved:** Teena Piccione (Mar 29, 2025 08:16 EDT) 03/29/2025

North Carolina State Chief Information Officer

| | Access Control Policy | Document No. SCIO-SEC-301 |
|---|---|---|

| Effective Date | Review Date | Version | Page No. |
|---|---|---|---|
| 01/29/2018 | 3/26/2025 | 4 | 1 of 23 |

## 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, and 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 who utilize State of NC IT resources are responsible for adhering to this policy and any local Access Control 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 the continued development, implementation, dissemination, and maintenance of information security policies, procedures, security controls and control techniques to address the Access Control process. Responsible for ensuring that the approved administrative and technical privacy controls are in place and effective. Responsible for educating employees about their access control responsibilities. |
| **Information Security** | The Information Security function is responsible for the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability |

| | |
|---|---|
| **Agency Security Liaison** | The Agency Security liaison is responsible for ensuring that security risks are managed in compliance with the State's requirements by collaborating with organizational entities. Liaisons are responsible for ensuring that the appropriate access controls are in effect for agency information systems. |
| **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 unauthorized access, use or modification of IT Resources (theft, fraud, or misuse of facilities). |
| **Third Parties** | Third party service providers must ensure that all IT systems and applications developed for the State conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures. |

## AC-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 Access Control security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the Access Control security principles established in the NIST SP 800-53, "Access Control" control guidelines as the official policy for this security domain. The "AC" designator identified in each control represents the NIST-specified identifier for the Access Control family. The following subsections in this document outline the Access Control requirements that each agency must implement and maintain in order to be compliant with this policy and to ensure that logical and physical access to information systems is sufficiently controlled. 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.
Organizations are required to implement necessary controls for providing authorized access and preventing unauthorized access to IT resources and information assets based on business and security requirements. All users of State and agency systems with access to non-public data must identify themselves and provide a means to authenticate their claimed identities appropriately for the risk level of the system and/or transaction. The policy statements in this document address the controls that will help to ensure that the State's IT resources and information assets are properly protected against unauthorized access, while meeting the access requirements for all authorized users. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in this policy.

Access to State information technology assets shall be controlled and managed to ensure that only authorized devices/persons have appropriate access in accordance with an agency's business needs. All computers that are permanently or intermittently connected to organizational networks shall have an approved credentials-based access control system. Regardless of the network connections, all systems handling Restricted and/or Highly Restricted data shall employ approved authentication credentials-based access control systems and encryption for data in transit. Access to systems shall be controlled by the following:

a. User profiles that define roles and access.

b. Revocation of access upon termination of employment.

c. Only authorized users shall be granted access to the State's information systems, and the principle of least privilege (see AC-6 Least Privilege) shall be used and enforced.

d. Assignment of privileges shall be based on an individual's job classification, job function, and the person's authority to access information. Job duties shall be separated as appropriate to prevent any single person or user from having any access not required by their job function.

e. Default access for systems containing Restricted or Highly Restricted data shall be deny-all.

f. Documented reviews shall be done for the following:

    i Standard users' rights, at least annually.

    ii Administrator/elevated user accounts every 6 months.

    iii General Physical Access:

    - Employee Badge/ID Card – Annually
    - Non-employee/contractor/vendor Badge/ID card – Quarterly

    ii. Secure Physical Access:

    - If access is given to secure physical area that contains FTI/SSA data, then the Badge/ID review to that secure physical area must be performed monthly regardless of employee type. See IRS 1075 Section 2.B.2 and 2.B.3.5 for more information.
    - If access is given to secure physical area that does NOT contain FTI/SSA data, then the Badge/ID review to that secure physical area must be performed quarterly regardless of employee type.

## AC-2 – Account Management

Policies and procedures shall be established for managing access rights for use of networks and systems throughout the life cycle of the user's credentials, such as user IDs, ID cards or badges, tokens, or biometrics. Access authorization includes the following appropriate requirements:

a. The types of accounts allowed and specifically prohibited for use within a system shall be defined and documented.

b. There shall be a documented approval process whereby authorized parties create user accounts and specify required privileges for user access to systems and data. Organizations shall require approval for requests to create information system accounts. Personnel or roles for requests to create information system accounts shall be defined.

c. Account managers shall be assigned for information systems. Backup system administrators shall also be identified to assist with user account management when the primary system administrator is unavailable.

d. Information system accounts shall be created, enabled, modified, disabled, and removed in accordance with documented organizational account management policy, procedures, prerequisites, and criteria.

e. User account policies and procedures including authentication procedures and requirements shall be communicated to all users of an information system.

f. User credentials shall be individually assigned and unique in order to maintain accountability. User credentials shall not be shared but only used by the individual assigned to the account, who is responsible for every action initiated by the account linked to that credential.

g. Default/generic credentials, such as “root” or “admin”, shall be disabled or changed prior to a system being put into production.

h. User credentials shall be disabled immediately upon the account owner’s termination from work or when the account owner no longer needs access to the system or application.

i. Conditions and criteria for group and role membership shall be established. Authorized users shall be specified for an information system, group, and role membership, as well as access authorizations (i.e., privileges) and other attributes (as required) for each account.

j. All systems must be assigned a system owner responsible for authorizing access.

k. The default access method for files and documents is role-based access control (RBAC), however, other methods to securely access files and documents may be used (e.g., attribute-based access control (ABAC), lattice-based access control (LBAC), etc.).

l. Access rights of users in the form of read, write, and execute shall be controlled appropriately and the outputs of those rights shall be seen only by authorized individuals.

m. Access to Restricted and/or Highly Restricted data shall be limited to authorized individuals who require access to the information as part of their job responsibilities.

n. An individual’s access to information technology assets shall be modified upon a change of employment or change in authorization, such as termination, a leave of absence or

temporary/permanent reassignment. An individual's access privileges may be changed, restricted, or eliminated *at any time*.

o. Only authorized system or security administrators or an authorized service desk staff shall be allowed to enable or re-enable a user credential except in situations where a user can do so automatically through challenge/response questions or other user self-service mechanisms.

p. All user credential creation, deletion and change activity performed by system administrators and others with privileged access shall be securely logged and reviewed on a regular basis.

q. User credentials established for a non-employee/contractor must have a specified expiration date unless a user credential without a specified expiration date is approved in writing by the agency security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.

r. Access control may need to be modified in response to the confidentiality, integrity or availability of information stored on the system, if existing access controls pose a risk to that information.

s. To facilitate intrusion detection, information shall be retained on all logon attempts until the agency determines the information is no longer valuable, or as required by law or the standards of this policy.

t. All authorized users of administrative-access accounts shall receive appropriate training on the use of those accounts.

u. Account management processes shall be aligned with personnel termination and transfer processes. For example, Human Resources shall ensure documented procedures exist for the immediate (or as applicable within approved time limits) notification of any termination (both voluntary and involuntary). This includes the notification of personnel role transfers/changes. This control ensures timely disabling or deactivation of system accounts by the agency-defined roles.

v. There shall be a process for notifying account managers when system accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need-to-know permission changes. The time-periods within which notifications to account managers should occur shall be specified for the following conditions:

    i. Accounts are no longer required,

    ii. When users are terminated / transferred,

    iii. When system usage/ need-know changes for an individual.

w. Access to information systems that receive, process, store, or transmit Federal Tax Information (FTI) shall be approved based on a valid access authorization, need-to-know permission, and under the authority to re-disclosed FTI under the provisions of IRC 6103.

x. The use of information system accounts shall be monitored. Accounts shall be reviewed for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts/roles. Privileged accounts are accounts with elevated

access and/or agency-defined roles assigned to individuals that allow those individuals to perform certain functions that ordinary users of that system are not authorized to perform. These privileged roles may include, for example, root access, system administrator access, key management, account management, network and system administration, database administration, and web site or server administration.

y. A process shall be established for reissuing shared/group account credentials (if deployed) when individuals are removed, for example, RACF accounts that are reissued to different individuals.

z. All accounts are processed for records management, litigation hold and other similar information disposition purposes prior to deleting, disabling, or transferring.

aa. Appropriate background checks shall be completed and adjudicated for unprivileged and privileged access and accounts according to Federal and/or State designation procedures for those systems that require it, for example, systems with FTI or Criminal Justice Information (CJI). In addition, N.C.G.S. § 143B-1336 (g) and N.C.G.S. § 143B-1379 (4) requires any employee or prospective employee of the Department of Information Technology and all agency security liaisons to be subject to a background investigation, including a criminal history record check, which may include a search of the State and National Repositories of Criminal Histories based on the person's fingerprints.

bb. Badge/ID cards shall be reviewed annually for employee general access and quarterly for secure access to a building. Non-employee/contractor badge/id cards shall be reviewed quarterly regardless of access type to a building.

## AC-2 (1) – Account Management | Automated System Account Management

Where technically configurable, organizational-defined automated mechanisms shall be employed to support the management of information system accounts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using system notification to report atypical system account usage.

## AC-2 (2) – Account Management | Automated Temporary and Emergency Account Management

Temporary and emergency accounts shall be immediately disabled or removed from a system using automated mechanisms once they are no longer needed. When temporary accounts are needed for internal or external audit, software development, software installation, training, guest access, or other defined need, automated mechanisms shall be used when applying the following conditions:

a. Authorized in advance by agency management,

b. Have a specific expiration date,
c. Be monitored while in use,
d. Be removed when the work is completed.

Training accounts shall be rendered inactive (e.g., by resetting the password) at the end of the training event. If multiple classes are held during a given day, the account may remain active until the end of the day, rather than resetting the accounts between classes held on the same day.

## AC-2 (3) – Account Management | Disable Accounts

User credentials that are inactive for a maximum of ninety (90) days must be disabled, except as specifically exempted by a security administrator. All accounts that have been disabled for greater than 365 days shall be deleted. Where technically configurable, the system shall automatically disable accounts per the conditions of this control.

If a non-employee/contractor badge/id card is not used to gain physical access to a building or the manager/sponsor does not approve the quarterly badge review, then the card will be disabled. If the badge is still disabled or not approved at the annual review, then the badge access shall be removed/deleted.

## AC-2 (4) – Account Management | Automated Audit Actions

Information systems shall automatically audit account creation, modification, enabling, disabling, and removal actions.

## AC-2 (5) – Account Management | Inactivity Logout

When users do not logout, an inactivity time-out period of 15 minutes shall be implemented. Individuals must physically log out or lock their device when they are expecting inactivity longer than the defined period of automatic enforcement of lockout (see AC-11). If there is someone in the vicinity of the user's system, while still logged on, there is risk of unauthorized individuals gaining access. See also NIST 800-63b section 4.3.3 Reauthentication.

## AC-2 (13) – Account Management | Disable Accounts for High-Risk Individuals

Accounts for high-risk individuals shall be disabled within a defined time period of any discovery of organization-defined risks. Organizations should define risk based on the likelihood and impact of the compromise of information assets. This is based on job role of the user that has access to those assets.

For instance, if there are job roles with access to critical systems/sensitive information, that is a high impact job role and a high-risk system. If there are threats of exfiltration and unauthorized disclosure of sensitive information (e.g., over social media), they should be defined and the risk identified. On discovery of inappropriate/prohibited activity, the accounts of high-risk individuals should be disabled immediately.

## AC-3 – Access Enforcement

The information system must enforce a role-based access control policy over defined subjects and objects and control access to the data based upon a valid access authorization, intended system usage, and the authority to disclose FTI under the provisions of IRC 6103. Password management requirements are described in the Identification and Authentication Policy, SCIO-SEC-307, Section IA-5.

## AC-4 – Information Flow Enforcement

Mechanisms shall be deployed to control access to the State's network backbone and/or routed infrastructure. The State Network must be configured to monitor and control communications at the external boundary of the network and internal boundaries at strategic locations. The State Network must connect to external networks or information systems only through managed interfaces approved by agency management. These managed interfaces must consist of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels, web content filters, data loss prevention) arranged in accordance with an effective, security architecture. Protective controls shall at a minimum include the following:

a. Positive source and destination address checking to restrict rogue networks from manipulating the State's routing tables.

b. Authentication to ensure that routing tables do not become corrupted with false entries.

c. Use network address translation (NAT) to obfuscate internal network addresses.

d. Email data leak prevention (DLP) to maintain compliance, identify and monitor the safe handling of specific categories of Restricted or Highly Restricted data as defined by N.C.G.S. 132-1.2, e.g., credit card numbers and U.S. social security numbers (SSNs).

e. Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to accomplish the mission of the agencies. Firewall configuration, installation, monitoring, and filtering requirements are found in the System and Communications Protection Policy SCIO-SEC-316, Section SC-7.

f. The information system shall enforce approved authorizations for controlling the flow of FTI within the system and between interconnected systems based on the technical safeguards in place to protect the FTI.

## AC-5 – Separation of Duties

Separation of duties is an integral part of a successful information security program that reduces the risk of accidental or deliberate system misuse. Separation of duties reduces opportunities for unauthorized modification or misuse of information by segregating the management and execution of certain duties or areas of responsibility. Management must ensure that there is proper segregation of duties to reduce the risk of system misuse and fraud.

a. Information system support functions (e.g., system management, programming, configuration management, quality assurance and testing, and network security) shall be conducted with different individuals.

b. System usage shall be monitored and reviewed for activities that may lead to business risks by personnel who are able to quantify and qualify potential threats and business risks. Appropriate controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task. Some events that should be monitored include over utilization of bandwidth, un-authorized login attempts, and un-authorized attempts to make changes to system settings.

c. System administration (e.g., access control functions) and system auditing shall be performed by different personnel.

e. System development and system change management shall be performed by different personnel.

f. System operations and system security administration shall be performed by different personnel.

g. If possible, security administration and security audit shall be performed by different personnel.

h. The responsibility for security audit shall be separate from other audit duties.

i. Activities that require collusion to defraud (e.g., exercising a purchase order and verifying receipt of goods) shall be identified, documented, and segregated.

j. Separation of duties is mandatory for all financial applications where misuse could cause a direct financial loss. Examples include, but are not limited to the following:

    i. Check issuance
    ii. Funds transfer
    iii. Input of vendor invoices
    iv. Other purchasing information
    v. Receiving information

Some additional examples of this principle include the following:

    i. The same individual shall not enter and authorize a purchase order.

ii. The same individual shall not request a user account and also create the account in the system.

iii. A system administrator shall not be the one to conduct the audits/reviews of the system he/she is administering.

iv. An Information Security Officer (ISO) shall not be a system administrator.

v. A Database administrator (DBA) shall have the minimum level of operating system rights necessary to create, edit and delete rights over the database specific files in the system directory, but no directory level rights in the system directory.

k. Development staffs (who have powerful privileges in the development environment) shall be prohibited from extending their administrative privileges to the operational environment.

l. Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and malicious code, e.g., trojan code.

## AC-6 – Least Privilege

The principle of least privilege shall be employed, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organization's missions and business functions. Least privilege applies to the development, implementation, and production lifecycle of information systems. The following shall be done.

a. Only authorized individuals shall perform updates to Restricted or Highly Restricted data such as citizen and business databases, protected health information (PHI), or FTI.

Authorized personnel include security administrators, system and network administrators, system maintenance personnel, system programmers, and other privileged users.

b. Information systems shall prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

i. Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.

ii. Non-privileged users are individuals that do not possess appropriate authorizations.

iii. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

c. Administrators of multi-user systems, systems that allow for concurrent usage of the system by multiple persons, must have at least two user credentials. One of these user credentials must provide privileged access, with all activities logged; the other must be a normal user credential for performing the day-to-day work of an ordinary user.

## AC- 6 (1) – Least Privilege | Authorize Access to Security Functions

Access to security functions and security-relevant information shall be explicitly authorized. Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

## AC- 6 (2) – Least Privilege | Non-Privileged Access for Nonsecurity Functions

Users of information system accounts, or roles, with access to sensitive information, shall use non-privileged accounts or roles when accessing non-security or non-privileged functions. This control enhancement limits exposure when operating from within privileged accounts or roles.

## AC-6 (5) – Least Privilege | Privileged Accounts

Privileged accounts on the information system shall be restricted to a limited number of authorized individuals with a need to perform administrative duties. Privileged accounts, including super user accounts, are typically described as system administrators for various types of systems.

a. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions.

b. Organizations may differentiate in an application between allowed privileges for local accounts and for domain accounts provided the organization retains the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

## AC-6 (7) – Least Privilege | Review of User Privileges

The following requirements shall be implemented to review user privileges:

a. Review of standard user accounts at least annually and privileged user accounts at east semi-annually; and

b. Reassign or remove privileges, if necessary, to correctly reflect agency mission and business needs.

## AC-6 (9) – Least Privilege | Log Use of Privileged Functions

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized entities that have compromised system accounts, is a serious and ongoing concern and

can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT).

Information systems shall log the execution of privileged functions as described in the Audit and Accountability Policy, SCIO-SEC-303, Section AU-2, Audit Events.

## AC-6 (10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Information systems shall prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

## AC-7 – Unsuccessful Logon Attempts

a. Where technically configurable, an information system shall limit unsuccessful logon attempts to three (3) during a 120-minute period before the user's account is disabled. For example, if an incorrect password is provided three (3) consecutive times, remote access systems shall drop the connection.

b. The locked-out duration shall be at least thirty (30) minutes unless the end user successfully unlocks the account through a challenge question scenario, or a system or security administrator, or an authorized service desk staff member re-enables the user's account. Also, a system or security administrator shall be notified when the maximum number of unsuccessful attempts is exceeded.

## AC-8 – System Use Notification

All network systems must use a logon banner containing State approved wording and must provide prompts as needed. Information system shall display to users a notification ***before*** granting access to the system that provides privacy and security notices consistent with applicable federal and state laws. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. The standard statewide logon banner is as follows:

*This is a government computer system and is the property of the State of North Carolina. This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system may subject the individual to administrative disciplinary actions, criminal and civil penalties. Users have no expectation of privacy. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result*

*in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.*

For systems that cannot accommodate the standard logon banner, the following 246-character wording may be used:

*This system is property of the State of North Carolina & is for authorized users ONLY. Unauthorized access may result in disciplinary action, civil & criminal penalties. Users have no expectation of privacy. USER EXPRESSLY CONSENTS TO MONITORING.*

For publicly accessible systems:

a. Displays system use information before granting further access;

b. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

c. Includes a description of the authorized uses of the systems

## AC-9 – Previous Logon (Access) Notification (Optional)

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

## AC-10 – Concurrent Session Control (Optional)

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

## AC-11 – Device Lock

The following shall be done:

a. The information system prevents further end user access to the system by initiating a device lock after 15 minutes of inactivity or upon receiving a request from a user.

b. The information system shall retain the device lock until the user reestablishes access using established identification and authentication procedures.

## AC-11 (1) – Device Lock | Pattern-Hiding Displays

Information systems shall conceal, via the device lock, information previously visible on the display with a publicly viewable image, such as a screen saver, photographic image, blank screen, solid colors, clock, etc. Screen saver images shall not convey sensitive information.

## AC-12 – Session Termination

A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an agency information system.

a. Network-connected single-user systems, such as laptops and PCs, shall employ agency-approved hardware or software mechanisms that control system booting and that include a time-out-after-no-activity (for example, a screen saver).

b. The time-out system must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. For some higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by agency policy, industry standard (e.g., PCI DSS) or other regulations.

## AC-13 – Supervision and Review | Access Control

Withdrawn: Incorporated into AC-2 and AU-6.

## AC-14 – Permitted Actions Without Identification or Authentication

Agencies shall determine what access controls are required, if any, for those specific instances where an agency determines that no identification and authentication is required for specific information systems. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred.

a. Users may access public websites or publicly available information on accessible State information systems without identification and authentication.

b. System/business owners, in collaboration with service provided, must identify, provide justification, and develop supporting documentation for user actions that can be performed on systems not requiring identification and authentication. Justification must specify the following:

   i. Actions that can be performed on the information system without identification and authentication may be permitted only to the extent necessary to accomplish Mission/Business Objectives.

   ii. Identification of responsible person for ensuring access control and monitoring is conducted.

iii. Supporting rationale for not requiring identification and authentication.

c. Compensating security controls shall be implemented at the directory and file level for all application specific and system accounts which do not require passwords. Implement only using least privilege, with access given only to necessary directories and files.

d. Restricted or Highly Restricted data may not be disclosed to individuals on the information system without identification and authentication and explicit authorization to such information.

## AC-15 – Automated Marking

Withdrawn: Incorporated into MP-3.

## AC-16 – Security Attributes (Optional)

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

## AC-17 – Remote Access

Where there is a business need and prior agency management approval, authorized users of agency computer systems, the State Network and data repositories shall be permitted to remotely connect to those systems, networks, and data repositories to conduct State-related business only through secure, authenticated and carefully managed agency approved access methods. Remote access is defined as access to State information by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet) that are not publicly accessible (e.g., agency LAN).

a. Access to State or agency data and resources via external connections from local or remote locations shall not be automatically granted with network or system access. Systems shall be available for on- or off-site remote access only after an explicit request is made by the user and approved by the manager for the system in question.

b. Usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed shall be established and documented.

c. Remote access to information systems shall be authorized prior to allowing such connections.

d. When unauthorized remote access is detected on State systems: (1) An alert shall be sent to appropriate system and security personnel, and (2) an alert is sent every hour thereafter until the device is removed from the network or authorized by the configuration management process.

e. Adequate security measures (e.g., virus and spam protection, firewall, intrusion detection) shall be required on client computers prior to allowing remote or adequately protected virtual private

network (VPN) access. Access to the State Network is a privilege and shall be denied, at the State CIO's discretion, to clients attached to networks deemed unacceptably vulnerable.

f. All users wishing to establish a remote connection via the Internet to an agency's internal network must first authenticate themselves at a firewall or security device.

g. Remote access for system administration functions that originate from networks external to the State Network, such as the Internet, must be accomplished, at a minimum, using multi-factor authentication (MFA).

h. Remote access to systems for end users, specifically for access to either Restricted or Highly Restricted data, shall be achieved using MFA technologies.

i. All users who require remote access privileges shall be responsible for the activity performed with their user credentials. User credentials shall never be shared with those not authorized to use those credentials. User credentials shall not be utilized by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user credentials belonging to others.

j. Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor, or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated upon an employee's or contractor's termination from service. Remote access privileges shall be reviewed upon an employee's or contractor's change of assignments and in conjunction with other regularly scheduled user account reviews.

k. Except for web servers or other systems where regular users are anonymous, users are prohibited from remotely logging into any state computer system or network anonymously (for example, using "guest" accounts). If users employ system facilities that allow them to change the active user ID to gain certain privileges, such as the switch user (su) command in Unix/Linux, they must have initially logged in with a user ID that clearly indicates their identity.

l. If a computer or network access control system is not functioning properly, it shall default to denial of access privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.

m. Split tunneling shall be disabled for all VPN solutions.

n. Remote access to single-equipment hosts (e.g., agency servers) shall be permitted provided the equipment requires authenticated access, is appropriately protected by a VPN, and prevents onward connection to the State Network.

o. Users requiring telecommunications access, such as dial-up modem access, for "out of band" management or special needs must obtain agency management approval.

## AC-17 (1) – Remote Access | Monitoring and Control

The information system shall use automated functions to monitor and control remote access methods. Systems shall log all remote access occurrences, including both end user and administrator activity (user credential, date/time, and duration of connection at a minimum). Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, laptops, smart phones, and tablets).

## AC-17 (2) – Remote Access | Protection of Confidentiality and Integrity Using Encryption

Encryption shall be implemented to protect the confidentiality and integrity of remote access sessions. Access through an agency-managed secure tunnel such as a Virtual Private Network (VPN) or Internet Protocol Security (IPSec) shall employ FIPS 140-2 compliant encryption techniques for encryption and secure authentication.

## AC-17 (3) – Remote Access | Managed Access Control Points

Remote access shall be routed through authorized and managed network access control points. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

## AC-17 (4) – Remote Access | Privileged Commands and Access

The execution of privileged commands and access to security-relevant information, e.g., logging into a firewall device for administrative functions, shall be authorized. Authorization shall occur in a format that provides assessable evidence and for agency defined needs. Remote access under these conditions shall be authorized only for compelling operational needs and the agency shall document the rationale for such access in the security plan for the system. Such actions shall be logged and audited.

## AC-18 – Wireless Access

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless devices include such things as laptops, smartphones, tablets, and Internet of Things (IoT) that access a network wirelessly. Each type of wireless access to the system shall be authorized prior to allowing such connections. To prevent eavesdropping by unauthorized personnel, various security measures shall be implemented including the following:

a. Access points shall be segmented from an organization's internal wired local area network (LAN) using a gateway device.

b. The SSID may indicate the name of the organization. The SSID name should be communicated to employees utilizing the wireless network (WLAN) to ensure they are connecting to the organization's network and not a rogue access point attempting to impersonate an official organizational WLAN.

c. A device must be prevented from connecting to a WLAN unless it can provide the correct SSID.

e. Every device used to access the State Network wirelessly, when not in use for short periods of time, shall be locked via operating system features. Devices shall be turned off when not in use for extended periods of time, unless the device is designed to provide or utilize continuous network connectivity (e.g., wireless cameras, RFID tag readers, and other portable wireless devices).

f. If supported, auditing features on wireless devices shall be enabled and the audits reviewed periodically by designated staff.

g. Endpoint protection systems shall be configured to disallow "dual-homed" wireless/wired connections, e.g., a laptop shall not be permitted to be connected to a State system via a wired connection while using a wireless connection to a non-State external system.

h. Authentication shall be performed when point-to-point wireless access points are used between routers to replace traditional common carrier lines.

i. A wireless intrusion detection/prevention system (e.g., WIPS) that access State resources shall be employed to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to an information system.

j. Security event logs for wireless networks connected to the State infrastructure shall be sent to a centralized log management tool.

k. Periodic war driving exercises shall be conducted in and around organizational facilities to detect unauthorized access points and ad hoc networks that are attached to the organization's network. Any unauthorized devices that are found shall be removed and reported through incident response procedures.

## AC-18 (1) – Wireless Access | Authentication and Encryption

a. Authentication and encryption technologies shall be used to protect wireless access to information systems.

   i. All wireless access to the State Network via an 802.11 wireless network shall be authenticated by requiring the user to supply the appropriate credentials as supported by the Wi-Fi directly or via the Extensible Authentication Protocol (EAP) extensions.

ii. Where a documented business case exists, user devices may authenticate using compliant service accounts but must require a user to re-authenticate to the Wi-Fi once the user has authenticated to the device.

iii. 802.1x credentials for individual users shall be deactivated in accordance with an agency's user management policy or within twenty-four (24) hours of notification of a status change (for example, employee termination or change in job function).

iv. Agency approved guest access shall give users access to only the Internet and shall use a captive portal that at least requires the guest users to agree to terms of service and states user activity on the wireless network is monitored.

b. FIPS 140-2 compliant encryption shall be used to protect wireless access to information system. For a list of validated cryptographic modules and products, refer to the following NIST publication: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

## AC-18 (3) – Wireless Access | Disable Wireless Networking

When not intended for use, wireless networking capabilities embedded within system components shall be disabled prior to issuance and deployment.

## AC-19 – Access Control for Mobile Devices

NIST defines a mobile device as a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source.

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, smartphones, tablets, e-readers, smart watches, digital cameras, and audio recording devices). Some of these devices are multifunctional and may be used for voice calls, text messages, email, Internet access, and may allow access to computers and/or networks. State resources and information shall be protected while using mobile communication devices through the following requirements:

a. Usage configuration/connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas shall be established and documented.

b. Connection of mobile devices to the organizational system shall be authorized prior to allowing such connections.

c. Mobile communication devices (personal or business owned) that are authorized to connect to state systems, such as email, shall require the following:

   i. A minimum 4-digit numeric, user defined, personal identification number (PIN) that is changed every 90 days.

   ii. A time out of inactivity that is 10 minutes or less.

   iii. If technically configurable, the ability to remotely erase the contents of the device, at the user's request, management request via a help desk service request, or by the user's own action. End users shall be made aware they are accepting the risk of personal data being lost.

d. Disable wireless functionality (i.e., Wi-Fi or Bluetooth) on appropriate devices that have wireless functionality (i.e., Wi-Fi or Bluetooth) when the device is not in use for an extended period of time.

e. Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones, and tablets). Laptop computers are excluded from this requirement.

f. Organizations shall comply with legal and regulatory requirements associated with information that is stored on the device, such as requirements for confidentiality, security, and record retention.

g. When unauthorized connections are detected, i) an alert shall be sent to appropriate system personnel, and ii) the device shall be isolated from the network.

h. Users shall adhere to the guiding principles and framework established in the Statewide Acceptable Use Policy (AUP).

## AC-19 (5) – Access Control for Mobile Devices | Full Device or Container-Based Encryption

Either full-device encryption or container encryption shall be employed to protect the confidentiality and integrity of information on organizational provided mobile devices. Where technically configurable, all data stored on mobile devices shall be encrypted.

## AC-20 – Use of External Information Systems

External information systems are information systems or components of information systems that are outside of the authorization boundary established by an organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, but are not limited to, the following examples: personally owned computers, personally owned mobile computing devices; privately owned computing and communications devices resident in commercial or public facilities

(e.g., hotels, convention centers, shopping malls, or airports); information systems owned or controlled by other governmental (Federal, State, or Local) organizations; and cloud computing services that are accessed from agency information systems.

a. Access to Restricted or Highly Restricted information from external information systems, other than through a virtual private network (VPN) is prohibited.

b. The use of personally owned devices with access to FTI may be allowed, without notification, only for the following purposes:

   i. Bring Your Own Device (BYOD) used to access e-mail, where all requirements in IRS 1075 are met.

   ii. Remote access through a virtual desktop infrastructure (VDI) environment, where all requirements in IRS 1075 are met.

c. Use of non-agency-owned information systems, system components, or devices to process, store, or transmit Restricted or Highly Restricted data requires agency-pre-approval prior to implementation.

d. Require that Cloud Service Providers (CSPs) configure systems such that access is consistent with defined, documented, and approved user access requirements, roles and responsibilities and account privileges and adhere to the following:

   i. System accounts and access are reviewed at least monthly to ensure that only the appropriate levels of access are allowed.

   ii. Access is granted only to authorized personnel.

   iii. Users' access rights are limited to least privilege.

## AC-20 (1) – Use of External Information Systems | Limits on Authorized Use

Authorized individuals shall be permitted to use an external information system to access the information system or to process, store, or transmit State data only when the organization does one of the following:

a. Verifies the implementation of required security controls on the external system as specified in the agency's information security policy and security plan; or

b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors) need to access agency information systems. In those situations, organizations need confidence that the external information systems contain the necessary security

controls so as not to compromise, damage, or otherwise harm their information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

## AC-20 (2) – Use of External Information Systems | Portable Storage Devices – Restricted Use

The use of agency-controlled portable storage devices by authorized individuals on external information systems shall be restricted using agency-defined restrictions. Limits on the use of agency-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

## AC-21 – Information Sharing

Restricted and Highly Restricted data shall be protected while utilizing software or information systems.

a. Organizations that share data or systems must have written agreements that address the business, security and technical requirements regarding the use and custodial responsibilities of the data and systems. These agreements can take the form of 1) a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), Service Level Agreement (SLA), or equivalent contractual agreement, and an Interconnection Security Agreement (ISA) or 2) a combined agreement.

b. If the sharing of data or systems is between two state agencies as part of a service, and not otherwise governed by legal requirements, the agencies may choose to use a Service Level Agreement (SLA) that clearly defines the responsibilities, services, priorities, and performance metrics of the services to be provided.

c. Agency software or information systems that allow the sharing of files and data containing Restricted and/or Highly Restricted information shall be used to share data only if the appropriate security controls are properly configured and implemented.

d. Appropriate security controls shall include the following:

    i. Authentication controls to ensure that authorized users are identified.

    ii. Access controls to limit an individual's access to only the Restricted and/or Highly Restricted data necessary for that person to perform his/her role.

    iii. Authorization controls to enforce version control and record retention requirements such that only designated individuals are able to modify or delete sensitive or critical records.

    iv. Audit controls that record individual actions on files and records, such as file modification.

v. Audit logs shall be retained in accordance with the agency records retention policy or the General Schedule for State Agency Records, Information Technology Records.

vi. These controls may be supplemented by operating-system-level controls (e.g., file and directory access control lists and system audit logs).

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

## AC-22 – Publicly Accessible Content

Business owners must do the following:

a. Designate individuals as authorized to post information onto publicly accessible information systems.

b. Train designated individuals to ensure that publicly accessible information does not contain non-public information.

c. Review the proposed content of publicly accessible information to ensure non-public information is not included prior to posting onto the information system.

d. Review content on the publicly accessible information system for non-public information and remove such information if discovered.

e. Content shall be reviewed at a minimum quarterly for the identification and removal of non-public data.

## AC-23 – Data Mining Protection (Optional)

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

## AC-24 – Access Control Decisions (Optional)

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

## AC-25 – Reference Monitor (Optional)

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.

| | | | |
|---|---|---|---|
| | **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.<br>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.

## 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 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 who utilize State of NC IT resources are responsible for adhering to this policy and any local Audit and Accountability 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 the continued development, implementation, dissemination, and maintenance of Audit and Accountability policy, procedures, security controls and control techniques. Ensures that personnel with significant responsibilities for system audit requirements are trained. |
| **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 system audit and accountability process requirements 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. |
| **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 enable the timely audit of system activities to reduce the risk of compromise of information or information systems managed by the State. |
| **Third Parties** | Third party service providers must provide Information Security Audit capabilities that meet State requirements. Third parties are required to maintain system audit controls and are subject to periodic review of audit accountability controls by the State. |

## AU-1 –Audit and Accountability 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 Audit and Accountability security controls at the organization, process and/or system level for all information assets / State data. This policy provides requirements for the audit and accountability process which is required to document, respond to, and minimize the impact of incidents that can impact information systems and data of which the State is considered the owner.

The State has adopted the Audit and Accountability security principles established in NIST SP 800-53, "Audit and Accountability" control guidelines as the official policy for this security domain. The "AU" designator identified in each control represents the NIST-specified identifier for the Audit and Accountability control family. The following subsections in this document outline the Audit and Accountability requirements that each agency must implement and maintain in order to be compliant with this policy. The objective of this policy is to assure that there is information and information system audits to account for, respond to, and minimize the impact of incidents that can impact the State's information or information systems. This policy and associated procedures shall be reviewed and updated annually, at a minimum. It 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.

## AU-2 – Event Logging

An audit event is any observable occurrence in an information system that is significant and relevant to the security of information systems and the environments in which those systems operate.

Organizations shall detect these events and protect the integrity and availability of information systems by monitoring operational audit logs.

a. Implement a program for continuous monitoring and auditing of system use to detect unauthorized or unusual activity.

b. All network components and computer systems used for agency operations must have the audit mechanism enabled and shall include logs to record specified audit events.

c. Audit logs for information systems containing Restricted and Highly Restricted data must be audited at the operating system, software, and database levels.

d. A current, reliable baseline shall be established that can be compared to audit logs to determine whether any abnormalities are present.

e. Server, desktop, and laptop computers shall be configured to audit for the following events:

   i. Server startup and shutdown

   ii. Starting and stopping of audit functions

   iii. Loading and unloading of services

   iv. Installation and removal of software

   v. System alerts and error messages

   vi. Application alerts and error messages

   vii. Modifications to the application

   viii. User logon and logoff

   ix. System administration activities, such as windows “runas” or linux “su” use.

   x. Accesses to information, files, and systems

   xi. Account creation, modification, or deletion

   xii. Password changes

   xiii. Modifications of access controls, such as change of file or user permissions or privileges (e.g., use of suid/guid, chown, su)

   xiv. Additional security-related events, as required by the system owner or to support the nature of the supported business and applications

   xv. Clearing of the audit log file

   xvi. Remote access outside of the agency network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system

xvii. Changes made to an application or database by a batch file

xviii. Application-critical record changes

xix. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)

xx. All system and data interactions concerning federal tax information (FTI)

f. Network devices (e.g., router, firewall, switch, wireless access point) shall be configured to audit for the following events:

i. Device startup and shutdown

ii. Administrator (e.g., privileged user) logon and logoff

iii. Configuration changes

iv. Account creation, modification, or deletion

v. Modifications of privileges and access controls

vi. System alerts and error messages

Audited events shall be reviewed and updated annually or when a major change to the information system occurs. Over time, the events an organization believes should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

## AU-3 – Content of Audit Records

Information systems shall be configured to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, the following elements shall be identified within each audit record:

a. Date and time when the event occurred

b. Software/hardware component of the information system where the event occurred

c. Source and destination network addresses

d. Source and destination port or protocol identifiers

e. Type of event that occurred

f. Subject identity (e.g., user, device, process context)

g. The outcome (i.e., success or failure) of the event

h. Security-relevant actions associated with processing

## AU-3 (1) – Content of Audit Records | Additional Audit Information

System Owners and Business Owners, in coordination for system residing off state infrastructure, shall ensure service providers configure information systems to generate audit records containing the following additional elements:

a. Manufacturer-specific event name / type of event

b. Full text recording of privileged commands

c. Individual identities of group account users

## AU-4 – Audit Storage Capacity

Audit record storage capacity must be allocated to retain audit records for the required audit retention period of two years per the requirement stated in the NC Department of Natural and Cultural Resources State's General Schedule for State Agency Records. This is to provide support for after-the-fact investigations of security incidents and to meet regulatory and State information retention schedule requirements.

a. Processing and storage capacity requirements shall be sufficient to capture and store the events cited above without adversely impacting operations.

b. On-line audit logs shall be backed-up to protected media well before the on-line logs are filled to capacity so that no audit information is lost or overwritten.

c. For information systems containing FTI, sufficient audit record storage capacity must be allocated to retain audit records for the required audit retention period of seven (7) years.

## AU-5 – Response to Audit Processing Failures

In the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded, the following requirements shall be met:

a. Alerts must be immediately sent to agency defined personnel or roles.

b. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator.

c. The system shall provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.

d. The system should automatically alert designated officials in the event of an audit failure or when audit capacity is 70%, 80%, and again at 90% utilization. This alert should be sent by a mechanism that allows system administrators to receive it after hours (e.g., email, text message).

e. Once the maximum storage capacity for audit logs is reached or there is an audit failure, the information system should overwrite the oldest audit records or automatically shut down to eliminate the chance of an incident, in the absence of auditing and accountability.

## AU-6 – Audit Record Review, Analysis, and Reporting

Unauthorized or unusual activity shall be detected by monitoring operational audit logs in order to protect the integrity and availability of information systems.

a. Staff shall be designated to regularly review operational audit logs, including system, application, and user event logs, for abnormalities.

b. Any abnormalities and/or discrepancies between the logs and the baseline that are discovered shall be reported to agency management.

c. Access to audit logs shall be restricted to only those authorized to view them, and the logs shall be protected from unauthorized modifications, and if technically configurable, through the use of file-integrity monitoring or change-detection software.

d. Review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of potentially unauthorized or unusual activity.

e. For systems containing FTI, refer to 4.3 Audit and Accountability in IRS 1075.

## AU-6 (1) – Audit Review, Analysis, and Reporting | Automated Process Integration

Automated mechanisms shall be employed to integrate audit review, analysis, and reporting processes, for example security information and event management (SIEM), to support agency processes for investigation and response to suspicious activities. Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and State Auditor audits.

## AU-6 (3) – Audit Review, Analysis, and Reporting | Correlate Audit Repositories

Audit records shall be analyzed and correlated across different repositories to gain organizational-wide situational awareness. Organizational-wide situational awareness includes awareness across all three tiers of risk management (e.g., organizational, mission/business process, and information system) and supports cross-organization awareness.

## AU-7 – Audit Reduction and Report Generation

Audit reduction and report generation capability shall be provided and implemented that does the following:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents

b. Does not alter the original content or time ordering of audit records.

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

## AU-7 (1) – Audit Reduction and Report Generation | Automatic Processing

a. Information systems shall provide and implement the capability to process audit records for events of interest based on AU-2. Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.

b. Audit event criteria may be defined to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.

## AU-8 – Time Stamps

Internal system clocks shall be used to generate time stamps for audit records. The internal system clocks should also be used to record time stamps for audit records that meets a NC Department of Information Technology (DIT) defined time synchronization and source; and that use either Coordinated Universal Time or that include the local time offset as part of the time stamp.

## AU-8 (1) – Time Stamps | Synchronization with Authoritative Time Source

Information systems shall synchronize internal information system clocks at an organizational-defined frequency to a DIT-defined authoritative time source. This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

## AU-9 – Protection of Audit Information

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion. Protection controls include the following:

a. Writing audit trails to hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R).

b. Backing up audit records onto a physically different systems or system component than the system or component being audited.

c. Writing audit files to a log server on the internal network and subsequently backing them up to a secure location.

d. Using cryptographic mechanisms to protect the integrity of audit information and audit tools. Cryptographic mechanisms include, for example, signed hash functions using asymmetric cryptography which allows verification of the hash information.

e. Enforcing dual authorization for movement and deletion of audit information for information systems containing Restricted and Highly Restricted data.

f. Alerting organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

## AU-9 (4) – Protection of Audit Information | Access by Subset of Privileged Users

Access to management of audit functionality shall be authorized to an organizational-defined subset of privileged users. Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records.

Access to manage audit functionality must be authorized only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries.

## AU-10 – Non-repudiation (Optional)

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

## AU-11 – Audit Record Retention

a. Information systems shall retain audit records for at least two (2) years per the requirement stated in the NC Department of Natural and Cultural Resources State's General Schedule for State Agency Records, Information Technology Records. This is to provide support for after-the-fact investigations of security incidents and to meet regulatory and State information retention schedule requirements.

b. For FTI, audit records for the events identified in AU-2 must be retained for seven (7) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

c. Audit records associated with known incidents, including those used for legal action, must be maintained in accordance with the State's record retention schedule after the incident is closed.

d. Agencies shall dispose of audit records when the retention time has expired, in accordance with the State's or IRS (for FTI information systems) record retention schedule after an incident is closed.

## AU-12 – Audit Record Generation

Organizations shall have the ability to generate audit records to monitor use of information systems by employee and third-party contractor users. The following shall be done:

a. The information system must provide audit record generation capability for the list of events to be logged defined in AU-2. Designated personnel can select which auditable events are to be audited by specific components of the system and generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

b. Information systems shall be configured to provide audit record generation capability for the list of auditable events defined in AU-2 with content prescribed in AU-3 on, at a minimum, the following information system components:

   i. Server, desktop, and laptop computers (file and print, web, firewalls, end-user environment)

   ii. Network components (e.g., switches, routers wireless)

## AU-13 – AU-16 (Optional)

These controls are not selected 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.

| | | | |
|---|---|---|---|
| | **Assessment, Authorization and Monitoring Policy** | | **Document No.** SCIO-SEC-304 |
| **Effective Date** 01/29/2018 | **Review Date** 03/26/2025 | **Version** 4 | **Page No.** 1 of 11 |

## 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.

This policy document provides the State of North Carolina's (State) security policy statements for the security assessment and authorization process for the effective and secure management of logical access to information systems and data of which the State is considered the owner.

## 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

Covered personnel performing designated roles in the security assessment and authorization process are responsible that the processes are executed and maintained in compliance with State and local agency policies in order to ensure that access to information assets is appropriate to the job responsibilities of every individual interacting with State owned information assets.

| 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 the continued development, dissemination, implementation, operation and monitoring of the Assessment and Authorization program. |

| | |
|---|---|
| **Enterprise Security Risk Management Office (ESRMO)** | The ESRMO is responsible for providing an enterprise approach to optimizing information technology (IT) security and risk management activities performed at the state and agency level. |
| **Management** | Management is responsible for documenting, tracking and reporting on the security state of agency information systems through the security authorization process. They may designate individuals to fulfill specific roles and responsibilities within the agency risk management process. |
| **Assessment and Authorization Personnel** | All covered personnel are responsible for assessing and or authorizing information system access must follow all State and local agency policies and procedures that are required for the effective implementation and assessment of selected controls and control enhancements in the security assessment and authorization process. |

## CA-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 Assessment, Authorization and Monitoring security controls at the organization, process and/or system level for all information assets / State data. The Assessment, Authorization and Monitoring process is implemented to ensure compliance with State information security policies and is critical to minimizing the threat of breaches. Security assessments are conducted to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Authorization is the process of accepting the residual risks associated with the continued operation of a system and granting approval to operate for a specified period of time.

Authorization to operate State information technology assets shall be controlled and managed to ensure that only authorized systems including workstations, servers, cloud computing applications, software applications, mobile devices, networks, and data repositories are implemented in accordance with an agency's business needs. It is the purpose of this policy to document the security assessment and authorization process 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 Assessment, Authorization and Monitoring principles established in NIST SP 800-53 "Assessment, Authorization and Monitoring," control guidelines, as the official policy for this security domain. The "CA" designator identified in each control represents the NIST-specified identifier for the Assessment, Authorization and Monitoring control family. The following

subsections in this document outline the Security Assessment and Authorization requirements that each State information system must implement and maintain 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.

## CA-2 - Control Assessments

Risk associated with each business system shall be assessed to determine what security requirements are applicable. Organizations shall select the appropriate assessor or assessment team for the type of assessment to be conducted. The control assessment determines the appropriate placement of each system and application within the security framework and evaluates the network resources, systems, data, and applications based upon their criticality. As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase. Control assessments must observe the following requirements:

1.1.1. Controls must be assessed under a Continuous Monitoring Plan supporting a frequency defined by the State Chief Information Security Officer (SCISO) for at least once every three (3) years, or when significant changes are made to the system or supported environment; and until the system is decommissioned.

1.1.2. The Continuous Monitoring plan shall be reviewed and approved by the State Chief Information Security Officer (SCISO) or designated representative prior to conducting the assessment.

a. Agencies shall provide to the State CIO their annual compliance and assessments reports, no later than September 1 of the given Calendar Year (CY). This certification includes compliance of cloud service providers. Any deficiencies identified within the agency which would preclude them from being compliant, must be addressed using the Corrective Action Plan (CAP) template. Reports must be submitted using approved secure methods.

b. Annual reports must ensure the agency has identified their security deficiencies and estimated cost for remediation. The report may include, but is not limited, to the following:

   i. Security boundary devices, e.g., firewalls, intrusion detection/prevention systems (IDPS)
   ii. Vulnerability management e.g., scanning, and patching systems
   iii. Resource constraints
   iv. Cybersecurity training deficiencies
   v. System development lifecycle (SDLC) deficiencies

d. When changes are made to an information system, a Security Impact Analysis shall be conducted to determine the extent to which changes to the information system will affect the security state of the system. These analyses are conducted as part of the System Development Lifecycle (SDLC) to ensure that security and privacy functional (and nonfunctional) requirements are identified and addressed during the development and testing of the system.

e. Agencies shall follow the procedures below when significant changes are made to the information system:

   i. Document assessment results and include correction or mitigation recommendations, to enable risk management and oversight activities.

   ii. Provide the assessment results to the ESRMO within thirty (30) days from the completion of the assessment.

   iii. The controls in the information system will be assessed on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system.

   iv. Cloud vendors must provide as an attestation of compliance via an independent third-party assessment report. Approved report types that meet the statewide requirement are provided in CA-7 of this policy. State agencies may include more restrictive requirements beyond the statewide requirement such as assessments that are performed against the Statewide Information Security Manual (SISM) and/or agency defined policies, standards, and other additional controls.

## CA-2 (1) - Control Assessments | Independent Assessors

Third third-party assessors or assessment teams shall be employed to conduct control assessments. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of information systems. Assessor independence provides a degree of impartiality to the process. To achieve impartiality, assessors should not do the following:

a. Create a mutual or conflicting interest with the organizations where the assessments are being conducted;

b. Assess their own work;

c. Act as management or employees of the organizations they are serving;

d. Place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments are typically contracted from public or private sector entities outside of the organization. This may include the NC National Guard Computer Network Defense (CND) Team.

## CA-3 - Information Exchange

All information systems must use approved and managed information exchange from the information system to other information systems that do the following:

a. Information exchange using Interconnection Security Agreements (ISAs), business associate agreement (BAA), or service level agreement (SLA), etc.

b. As part of each exchange agreement, document the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, costs incurred under the agreement and the nature of the information communicated.

c. Employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit data to connect to external information systems.

d. Monitor the information assets connections on an annual basis verifying enforcement of security requirements.

e. Follow the procedures below for connections to systems outside of the State Network:

   i. Establish an approved Memorandum of Understanding / Agreement (MOU/A) or Interconnection Security Agreement (ISA) signed by the State Chief Information Officer (SCIO) or designee or Agency CIO.

   ii. Submit a connection request as well as a Privacy Threshold Analysis (PTA) document to the Department of Information Technology (DIT). The request shall include the following:

      1. Type of connection to be established
      2. Type Connection requirements
      3. Key personnel to help coordinate the planning efforts of the system interconnection
      4. Duration of the interconnection
      5. Point of contact for the external organization requesting the interconnection of data and level of sensitivity of the data being exchanged.

   iii. Prior to system interconnection, system owners must complete a security impact analysis. The results must be provided to the Agency CIO for risk determination and approval.

   iv. Review and update ISAs at minimum annually or whenever there is a significant change to any of the interconnected systems.

   v. Terminate all interconnections when any of the following conditions are met:

      1. The ISA, MOU/MOA or SLA has expired or is withdrawn

2. The business requirement for the interconnection no longer exists
3. A significant change in the environment increases the risk to an unacceptable level of operations

**Note:** This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as website browsing.

## CA-3 (5) - Information Exchange | Restrictions on External System Connections

All systems containing Restricted or Highly Restricted data shall have restrictions for connecting to external information systems. Organizations can constrain information system connectivity to external domains (e.g., websites) by employing deny-all, allow by exception policy, also known as whitelisting. Organizations determine what exceptions, if any, are acceptable.

## CA-4 – Security Certification

Withdrawn: Incorporated into CA-2.

## CA-5 – Plan of Action and Milestones/Corrective Action Plan

When deficiencies are discovered in the security posture of systems, a Plan of Action and Milestones (PO&AM) or Corrective Action Plan (CAP) shall be developed for such information systems that does the following:

a. Document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system.

b. Update existing action plans and milestones based on the findings from controls assessments, independent audit reviews, and continuous monitoring activities.

c. All discovered weaknesses, recommendations and their sources of discovery shall be traceable to the related CAP. Agency Security Liaisons shall review and validate completed CAPs to ensure that artifacts are in place supporting the closure, those CAPs not meeting criteria to close shall be returned to the security liaison for remediation and resubmission for closure.

d. The following information shall be included in each CAP:

   i. Type of weakness

   ii. Identity of the Agency, Division, Office responsible for resolving the weakness

iii. Estimated funding required for resolving the weakness

iv. Scheduled completion date for weakness remediation or mitigation

v. Key milestones with completion dates

vi. Source of weakness discovery

vii. Status of the corrective action, e.g., Ongoing or Completed

viii. Security Incidents

e. Identify and document any SCIO or delegate's decision to accept a weakness in a CAP.

f. CAPs must be reviewed and updated at minimum quarterly.

g. Identified weaknesses must be analyzed to determine level of risk, (e.g., high, medium, low)

h. Document weaknesses in an EGRC tool based on the following timelines:

i. Weaknesses identified as High must be entered if they cannot be remediated or mitigated within 30 days of discovery.

ii. Weaknesses identified as Medium must be entered if they cannot be remediated or mitigated within 60 days of discovery.

iii. Weaknesses identified as Low must be entered if they cannot be remediated or mitigated within 90 days of discovery.

iv. All remediated or mitigated weaknesses must have supported artifacts, e.g., screenshots, scan results etc.

## CA-6 – Authorization

a. All information systems must have a senior-level executive (such as an Agency CIO or delegate), who is responsible for the information asset and authorizing the use of common controls available for inheritance by the information asset. The senior-level executive will ensure the following:

i. Ensure that the responsible individual accepts the use of common controls inherited by the system and authorizes the information asset for processing, e.g., Authority to Operate (ATO), before the system commences operations.

ii. Ensure the information system meets State, Federal and other mandates for compliance on an annual basis.

iii. Authorization levels shall be reviewed and updated regularly to prevent disclosure of information through unauthorized access.

b. All responsible parties shall consider whether granting authorization for an individual to use a system utility, (e.g., disk cleanup, disk defragmenter, system restore, disk compression and archival) may violate segregation of duties if the utility allows bypassing or overriding of segregation controls. If granting authorization to use a system utility could potentially violate segregation controls, the agency shall enact precautions to ensure that this violation does not occur. Detailed auditing or two-person control could provide assurance that segregation of duties is maintained. System utility misuse can cause the deletion or movement of files, the deletion of system restore points, or cause errors to occur in registry files.

c. System documentation and user procedures shall be updated to reflect changes based on the modification of applications, data structures and/or authorization processes.

d. Access shall require authentication and authorization to access needed resources, and access rights shall be regularly reviewed.

## CA-7 – Continuous Monitoring

A program for system-level continuous monitoring and auditing of system use shall be implemented to detect unauthorized or unusual activity. The system-level continuous monitoring program should support the organization-level continuous monitoring strategy. This includes systems that are cloud hosted by contracted vendors or agency managed. All hardware connected to the State Network or cloud hosted shall be configured to support State/agency management and monitoring standards.

All organizations must complete an annual risk and security assessment of their critical systems and infrastructure and ensure that there are ongoing processes in place to assess the current posture of the environment. Continuous Monitoring is a program that ensures that all agencies are assessed annually at a minimum. The Continuous Monitoring program includes the following:

a. A configuration management process for the information system and its constituent components.

b. A determination of the security impact of changes to the information system and environment of operation.

c. Ongoing control assessments in accordance with the Continuous Monitoring Plan must include the following:

   i. Performance metrics concerning the status of control compliance and corrective actions required for identified control gaps;

   ii. Development of a process to evaluate supporting documentation;

   iii. The time required to monitor assessment recommendations;

iv. A schedule for assessing critical systems on an annual basis;

v. Security and Privacy status results reporting to be provided to ESRMO within 30 days of completion of an assessment through a corrective action plan (CAP);

vi. Coordination between the agencies and the ESRMO to address residual risks for those controls that cannot be implemented.

d. Business Owners and System Owners, in coordination with Agency CIOs, CISOs and Security Liaisons for State data residing in non-state locations, e.g., cloud or off-site hosted systems, shall ensure service providers do the following:

i. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor ***prior*** to contract approval.

ii. Implement the Continuous Monitoring Plan.

iii. For vendor hosted systems/solutions that will have Restricted or Highly Restricted data, agencies shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Examples of acceptable attestation reports include Federal Risk and Authorization Management Program (FedRAMP) certification, Service Organization Controls (SOC 2) Type 2, ISO/IEC 27001:2022 Information Security Management Standard, and HITRUST CSF (Common Security Framework). In addition, vendors must provide the agency an industry recognized, third party assessment report annually for the duration of the contract.

**Note**: SaaS vendors cannot use IaaS/PaaS certifications unless the application is explicitly covered as part of those assessments.

iii. Correlate and analyze system level security-related information generated by assessments and monitoring to identify weaknesses and develop corrective actions.

iv. Report system level security and privacy status to the ESRMO through an EGRC repository, if available.

v. Demonstrate to the State that ongoing continuous monitoring activities are in place and compliance is being met for the following requirements:

1. Security
2. Privacy and Confidentiality
3. Availability (Business Continuity Management)
4. Processing integrity

## CA-7 (1) – Continuous Monitoring | Independent Assessment

Third-party independent assessors or assessment teams shall be employed to monitor the controls in information systems on an ongoing basis. An independent 3rd party assessor is an entity separate from the agency and/or vendor that is being accessed and can provide an objective opinion on an information system. Organizations can maximize the value of assessments of system controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Refer to CA-2 (1) - Control Assessments – Independent Assessors for more information.

## CA-7 (4) Continuous Monitoring | Risk Monitoring

Risk monitoring is informed by the established organizational risk tolerance. Risk monitoring shall be an integral part of the continuous monitoring strategy / plan. The plan shall include the following:

a. Effectiveness monitoring, which determines the ongoing effectiveness of the implemented risk response measures.
b. Compliance monitoring, which verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied.
c. Change monitoring, which identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

## CA-8 – Penetration Testing

All systems containing Restricted or Highly Restricted data shall have a penetration test performed by an independent third-party assessor at least annually. This may be part of a third-party assessment/certification, e.g., SOC 2 Type 2.

Endpoint threat monitoring of all devices shall be required including services within the cloud.

This control is optional for LOW risk information systems.

## CA-9 – Internal System Connections

Security compliance checks must be performed between information systems and (separate) system components (e.g., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, internal connections for a class of components with common characteristics and/or configurations may be authorized, for

example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

For enterprise solutions, DIT shall do the following:

a. Establish classes and subclasses of components permitted for internal system connections.

b. Develop baseline configurations for each component class and subclass.

c. Define interface characteristics and security and privacy standards for each component class and subclass connection type by FIPS-199 categorization – Moderate or Low.

d. Terminate internal system connections after agency-defined conditions.

e. Review the continued need for each internal connection on an agency-defined frequency.

Agency Business/System Owners shall only implement the established classes and sub-classes of components according to baseline configurations and security and privacy requirements. Any deviations from standards must be submitted through the DIT Exception Process.

## 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.

## 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, and 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 who utilize State of NC IT resources are responsible for adhering to this policy and any local Configuration Management 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 the continued development, dissemination, implementation, operation and monitoring of the Configuration Management program. Ensures that personnel with significant responsibilities for configuration management are trained. |
| **Agency Security Liaison** | The Agency Security Liaison is responsible for ensuring that security risks are managed in compliance with the State's requirements by collaborating with organizational entities. Liaisons are responsible for ensuring the appropriate configuration management controls are in effect for agency information systems. |

| | |
|---|---|
| **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 configuration management for the information system 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. |
| **Covered Personnel** | Covered personnel must provide Configuration Management capabilities that meet agency requirements. Configuration Management practices are subject to periodic review by the agencies. |

## CM-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 Configuration Management security controls at the organization, process and/or system level for all information assets / State data. This document provides requirements for the configuration management 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 has adopted the Configuration Management security principles established in NIST SP 800-53, "Configuration Management" control guidelines as the official policy for this security domain. The "CM" designator identified in each control represents the NIST-specified identifier for the Configuration Management control family. The following subsections in this document outline the Configuration Management 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.

## CM-2 – Baseline Configuration

Common security configurations shall be made available that provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This requirement allows agencies to improve information system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of State data. The following shall be done:

a. A current baseline configuration must be developed, reviewed, approved, documented, and maintained under configuration control for each information system. The Department of Information Technology (DIT) shall be responsible for baseline configurations for enterprise solutions.

b. A baseline configuration must document and provide information about the components of an information system including the following:

   i. Standard operating system/installed applications with current version numbers

   ii. Standard software load for workstations, servers, network components, and mobile devices and laptops

   iii. Up-to-date patch level information

   iv. Network topology

   v. Logical placement of the component within the system and enterprise architecture

   vi. Technology platform

c. New baselines must be created as the information system changes over time to maintain the baseline configuration.

d. Ensure product versions of technologies are kept up to date and the latest security patches are applied.

   Agencies will ensure “best effort” to maintain all information technologies within N-1, where “N” is a major version. At minimum all operating systems and primary applications shall be maintained at baseline security configurations of no less than N-2. All current security patches for information technologies shall be applied prior to deployment and shall be maintained as meets or exceeds the SI-2 Flaw Remediation control. Whereas, “best effort” means taking, in good faith, all reasonable steps to achieve the objective, carrying the process to its logical conclusion and leaving no stone unturned.

e. Utilize best practice system hardening baselines for the operating systems. Refer to CM-6 Configuration Settings for a list of approved baselines.

i. In cases where a baseline security configuration does not exist for an operating system, the State Chief Information Security Officer (SCISO) or designee shall ensure a baseline security configuration is developed, documented, and approved.

f. Document any exceptions to baseline security configurations and obtain approval by the SCRO or designee.

g. Maintain records confirming the implementation of baseline security configurations for each IT system they manage.

h. Review and update the baseline configuration for information systems:

   i. Annually, at a minimum

   ii. When required due to system upgrades, patches, or other significant changes have occurred in the baseline configuration

   iii. As an integral part of information system component installations and upgrades

   iv. When an increase in interconnection with other systems outside the authorization boundary or significant changes in the security requirements for the system

## CM-2 (2) Baseline Configuration |Automation Support for Accuracy and Currency

The currency, completeness, accuracy, and availability of the baseline configuration of the system shall be maintained using automated mechanisms such as the following:

a. Backup of individual configuration files, or similar method that allows for only the restore of the configuration

b. Snapshot systems or applications that may also allow for reviewing differences or compliance

c. Version control applications that are operated on a system separate from those being versioned

## CM-2 (3) – Baseline Configuration |Retention of Previous Configurations

Retain previous versions of baseline configurations of the information system to support rollback, for example, hardware, software, firmware, configuration files, and configuration records.

## CM-2 (7) Baseline Configuration | Configure Systems and Components for High-Risk Areas

All devices taken to high-risk areas external to the organization should be considered compromised upon return from those areas. They could contain malicious software that you do not want to introduce to the State's network or to your home network. Systems and components used for high-risk areas shall be configured as follows:

a. Issue organizational defined selected systems with defined configurations to individuals traveling to locations that the organization deems to be of significant risk. Refer to the International Travel Policy.

b. Have laptops, cellphones, and portable devices sanitized ***prior*** to travel.

c. Have devices that will be in high-risk areas securely erased and rebuilt, either from an existing backup or through a new installation of the operating system.

## CM-3 – Configuration Change Control

Changes to systems and application programs shall be managed to protect the systems and programs from failure as well as security breaches. Adequate management of system change control processes shall require the following:

a. Safeguard production systems during modification, including emergency changes.

b. Enforcement of formal change control procedures.

c. Proper authorization and approvals at all levels.

d. Successful testing of updates and new programs prior to their being moved into a production environment.

e. Determine and document the types of changes to the information system that are configuration controlled.

f. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.

g. Document configuration change decisions associated with the information system.

h. Implement approved configuration-controlled changes to the information system.

i. Retain records of configuration-controlled changes to the information system for the life of the system.

j. Monitor and review activities associated with configuration-controlled changes to the information system.

k. Coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur.

l. Test, validate, and document changes to the information system before implementing the changes on the system.

m. Ensure updates addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources.

Vulnerability Management requirements are addressed in the System and Information Integrity Policy SCIO-SEC-317, Section SI-2.

n. Integrate application change control and operational change control procedures. This effort should include the following processes, controls, and best practices:
   i Controls and approval levels for updating libraries
   ii Requiring formal agreement and approval for any changes
   iii Restricting library content
   iv Restricting programmers' access to only those parts of the system necessary for their work
   v Version control for each application.
   vi Tying program documentation updates to source code updates
   vii Audit logs that track all accesses to libraries, copying and use of source code, and updates posted to libraries
o. Define job responsibilities/restrictions and establishing authority levels for the following:
   i. Program librarian(s)
   ii. Developers (i.e., should neither test their own code nor promote it into production)
   iii. Other IT staff
p. Identify personnel authorized to make or submit changes to the source library (i.e., a program librarian) for each major application to control check-in/check-out.
q. Provide role-based training for business and technical users covering new features and security controls introduced by the upgrade.
r. Use rollback procedures designed to recover to previous stable version of programs.

## CM-3 (4) – Configuration Change Control | Security and Privacy Representatives

Organizational defined security and privacy representatives shall be members of the Configuration Control Board.

## CM-4 –Impact Analyses

When significant changes are planned for, or made to, a system, the system owners, agency security liaison or business owners for systems shall conduct impact analyses to determine which security and privacy controls shall be assessed for proper implementation and operation. An impact analysis may

include, for example, reviewing plans to understand security and privacy control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. The following risk impact analyses activities shall be incorporated into the documented configuration change control process:

a. Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for agency functions or services.

b. Identification of Restricted or Highly Restricted information, which are stored in the agency's files, and the potential for fraud, misuse, or other illegal activity. Data classifications are defined within the Statewide Data Classification and Handling policy.

c. Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical agency functions and services.

d. Identification of the processes used to monitor and report to management on whatever applications, tools, and technologies the agency has implemented to adequately manage the risk as defined by the agency (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).

e. Identification of the agency's IT Change Management and Vulnerability Assessment processes.

f. Identification of the security and privacy mechanisms that are in place to conceal agency data, for example the use of encryption, data masking, etc.

g. Changes shall be analyzed and evaluated for the impact on security and privacy preferably before they are approved and implemented.

h. Security and Privacy risk analysis requirements and definitions are addressed in the Risk Assessment Policy SCIO-SEC-314, Section RA-3.

## CM-4 (2) Impact Analyses | Verification of Controls

Organizations shall verify (after system changes) that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

## CM-5 – Access Restrictions for Change

Physical and logical access restrictions associated with changes to the information system shall be defined, documented, approved, and enforced. The following shall be done:

a. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

b. All requests for local administrative rights must be documented and approved by agency management.

c. Access records must be maintained to ensure that configuration change control is being implemented as intended and for supporting after-the-fact actions should the State become aware of an unauthorized change to an information system.

d. Privileges to change information system components and system-related information within a production or operational environment shall be limited to avoid unintended changes to other systems and business processed.

e. Use two-person integrity to ensure that changes to defined critical systems cannot occur unless both individuals implement such changes.

f. Restrict access to operating system and operational or production application software/program libraries to designated staff only.

## CM-6 – Configuration Settings

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. The following requirements shall be implemented:

a. A standard set of mandatory configuration settings must be established and documented for information technology components employed within the information system. Standard Configuration Documents (SCDs) must detail the configuration settings.

b. The selected configuration settings, whether State standards or designed specifically for the information system, must reflect the most restrictive mode consistent with operational requirements and must be derived from the following sources, listed in order of precedence:

   i. NIST recommended configurations and common secure configurations: https://ncp.nist.gov/repository

   ii. Defense Information Systems Agency (DISA) common secure configurations and Standard Technical Implementation Guides (STIGs): https://public.cyber.mil/stigs/downloads/

   iii. National Security Agency (NSA) configuration guides: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm

iv. Center for Internet Security (CIS) benchmarks: https://www.cisecurity.org/cis-benchmarks/

v. Safeguard Computer Security Evaluation Matrix (SCSEM): https://www.irs.gov/privacy-disclosure/computer-security-compliance-references-and-related-topics, for systems that store, process, or transmit federal tax information (FTI).

c. Identify, document, and approve any deviations from established configuration settings for information systems.

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

## CM-7 – Least Functionality

The following requirements shall be implemented to provide least functionality:

a. Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.

b. Where technically configurable, component functionality shall be limited to a single function per device (e.g., email server, web server, etc.).

c. Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure. Organizations can either decide the relative security of a function, port, protocol, and/or service or base a security decision on the assessment of other entities. The use of the following functions, ports, protocols, software and/or services, at a minimum, must be specifically prohibited or restricted:

i. ARINC-GATEWAY Port 55210 / TCP

ii. Background File Transfer Protocol (BFTP) Port 152 / TCP

iii. Border Gateway Protocol (BGP) Port 179 / Transmission Control Protocol (TCP)

iv. Courier Port 530 / TCP, User Datagram Protocol (UDP)

v. Domain Name System be (DNS) Port 53 / TCP, UDP

vi. File Transfer Protocol (FTP) Ports 20, 21 / TCP

vii. Finger Port 79 / TCP

viii. Hypertext Transfer Protocol (HTTP) Port 80 / TCP; 443 / TCP

ix. HTTP-MGMT Port 280 / TCP

x. Identification Protocol (IDENT) Port 113 / TCP, UDP

xi. Internet Control Messaging Protocol (ICMP) - block incoming echo request (ping and Windows traceroute) block outgoing echo replies, time exceeded, and destination

unreachable messages except “packet too big” messages (type 3, code 4). **Note:** Blocking ICMP will restrict legitimate use of PING to restrict malicious activity.

xii. Internet Message Access Protocol (IMAP) Port 143 / TCP, UDP

xiii. Internet Relay Chat (IRC) Port 194 / UDP

xiv. Lightweight Directory Access Protocol (LDAP) Port 389 / TCP, UDP

xv. Line Printer Daemon (LPD) Port 515 / TCP

xvi. LOCKD Port 4045 / TCP, UDP

xvii. Network Basic Input Output System (NetBIOS) Ports 135, 445 / TCP, UDP; 137-138 / UDP; 139 / TCP

xviii. Network File System (NFS) Port 2049 / TCP, UDP

xix. Network News Transfer Protocol (NNTP) Port 119 / TCP

xx. Network Time Protocol (NTP) Port 123 / TCP

xxi. Oracle Names (ORACLENAMES) Port 1575 / TCP, UDP

xxii. Port Mapper (PORTMAP/RPCBIND) Port 111 / TCP, UDP

xxiii. Post Office Protocol 3 (POP3) Ports 109-110 / TCP

xxiv. r Services Ports 512-514 / TCP

xxv. Secure Shell (SSH) Port 22 / TCP

xxvi. Session Initiation Protocol (SIP) Port 5060 / TCP, UDP

xxvii. Shell Port 514 / TCP

xxviii. SIDEWINDER-COBRA, (S) Port 2809 & 9002 / TCP

xxix. Simple File Transfer Protocol (SFTP) Port 115 TCP, UDP

xxx. Simple Mail Transfer Protocol (SMTP) Port 25 / TCP

xxxi. Simple Network Management Protocol (SNMP) Ports 161-162 / TCP, UDP

xxxii. Snare Port 509 / TCP, UDP

xxxiii. Socket Secure (SOCKS) Port 1080 / TCP

xxxiv. SOFTWAREAGWEBMETHODS Port 6849 / TCP

xxxv. Structured Query Language (SQL) Port 118 / TCP, UDP; Port 156 / TCP, UDP

xxxvi. Super Duper Telnet Port 95 / TCP

xxxvii. SYMANTEC-ITA Port 3833-3836 / TCP

xxxviii. Syslog Port 514 / UDP

xxxix. Telnet Port 23 / TCP

xl. TIME Port 37 / TCP, UDP

xli. TIMBUKTU Port 407 / TCP, UDP

xlii. Trivial File Transfer Protocol (TFTP) Port 69 / UDP

xliii. VNC-SERVER Port 5900 / TCP

xliv. X Windows Ports 6000-6255 / TCP

xlv. YAK-CHAT Port 258 / UDP

## CM-7 (1) – Least Functionality | Periodic Review

The following shall be done:

a. Review the system on a defined frequency to identify unnecessary and/or non-secure functions, ports, protocols, services, and applications; and,

b. Disable or remove unnecessary and/or non-secure functions, ports, protocols, services, and software.

## CM-7 (2) - Least Functionality | Prevent Program Execution

An information system shall prevent program execution in accordance with organizational-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.

This control is optional for LOW risk systems.

## CM-7 (5) – Least Functionality | Authorized Software

The following shall be done:

a. Identify organizational-defined software programs authorized to execute on the system.

b. Review and update the list of authorized software programs per an agency-defined frequency.

c. Where technically configurable, employ a deny-all, permit-by-exception policy for software executables on systems with Restricted or Highly Restricted data.

d. This control is optional for LOW risk systems.

## CM-8 – System Component Inventory

The following shall be done:

a. Develop, document, and maintain an inventory of information system components that accurately reflects the current information system environment.

b. Verify that all components within the system are not duplicated in other information system component inventories.

   Inventory all components within the authorization boundary of the information system (this may inter-connected systems). The inventory includes information deemed necessary to achieve effective property accountability and is at the level of granularity for tracking and reporting, for example, the following:

   i. hardware inventory specifications (manufacturer, type, model, serial number, physical location),

   ii. software license information,

   iii. information system / component owner(s),

   iv. associated component configuration standard,

   v. software/firmware version information, and

   vi. for a networked component/device, the machine name and network address,

c. Review and audit information system component inventory,

d. Include assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory,

e. Review and update the information system component inventory annually, at a minimum.

## CM-8 (1) – System Component Inventory | Updates during Installation and Removal

The inventory of information system components shall be updated as an integral part of component installations, removals, and information system updates.

## CM-8 (3) –System Component Inventory | Automated Unauthorized Component Detection

Automated mechanisms shall be defined and employed to detect the presence of unauthorized hardware, software, and firmware components within the information system. One or more of the following actions may be taken when unauthorized components are detected:

i. Disable network access to such components

ii. Isolate the components

iii. Notify agency-defined personnel

This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices.

## CM-9 – Configuration Management Plan

A configuration management plan shall be developed, documented, and implemented for information systems that does the following:

a. Addresses roles, responsibilities, and configuration management processes and procedures,

b. Defines the configuration items for the information system and when in the system development life cycle (SDLC) the configuration items are placed under configuration management,

c. Establishes the means for identifying configuration items throughout the SDLC and a process for managing the configuration of the configuration items,

d. Assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development. In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process,

e. Defines detailed processes and procedures for how configuration management is used to support SDLC activities at the information system level,

f. Describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated,

g. Creates a step-by-step implementation plan for every configuration change,

h. Requires that software implementation plans follow change control procedures,

i. Protects the configuration management plan from unauthorized disclosure and modification,

j. The configuration management plan approval process must include the following:

   i. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system

   ii. Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system

## CM-10 – Software Usage Restrictions

The following shall be done:

a. Provide employees, contractors and other third parties with guidelines for obeying software licensing agreements, to include open source software, and shall not permit the installation of unauthorized copies of software on technology devices that connect to the State Network.

   i. Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

   ii. Employees, contractors and other third parties shall use software and associated documentation in accordance with contract agreements and copyright laws.

   iii. Employees, contractors and other third parties who make, acquire, or use unauthorized copies of software shall be disciplined as appropriate. Such discipline may include termination.

   iv. Open source software must adhere to a secure configuration baseline checklist from the U.S. Government or industry.

b. Inform their users of any proprietary rights in databases or similar compilations and the appropriate use of such data.

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

d. Establish procedures for software use, distribution, and removal within an organization to ensure organizational use of software meets all copyright and licensing requirements. Procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

## CM-11 – User Installed Software

Only standard approved software shall be installed on State owned assets with any deviations being pre-approved by agency management and reviewed by an agency security liaison assigned to perform the review. The following shall be ensured for installed software:

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through automated methods, if available and technically configurable.

c. Monitor policy compliance quarterly, at a minimum.

d. Ensure only software programs that are from validated media are installed and are free of harmful code or other destructive aspects.

e. Refer to the Statewide Acceptable Use Policy (AUP) for additional requirements.

## CM-12 – Information Location

The following shall be done:

a. Identify and document the location of "organizational-defined information" and the specific system components on which the information is processed and stored.

b. Identify and document the users who have access to the system and system components where the information is processed and stored.

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

## CM-12 (1) – Information Location |Automated Tools to Support Information Location

Where technically configurable, automated tools shall be used to identify organizational-defined information by information type on system components to ensure controls are in place to protect organizational information and individual privacy.

## 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.

| | Contingency Planning Policy | Document No. SCIO-SEC-306 |
|---|---|---|

| Effective Date | Review Date | Version | Page No. |
|---|---|---|---|
| 01/29/2018 | 03/26/2025 | 4 | 1 of 10 |

## 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 who utilize State of NC IT resources are responsible for adhering to this policy and with any local Contingency Planning 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 the continued development, dissemination, implementation, operation and monitoring of the Contingency Planning program. |
| **Business Continuity Plan Administrator & Planner** | The person(s) designated as the agency Business Continuity (BC) & Disaster Recovery (DR) Plan Administrator and Planner(s) has the responsibility of overseeing the individual plans and files that constitute the BC/DR Plan and ensuring that they are current, meet these standards and are consistent with the agency's overall plan. At the direction of the State Chief Information Officer, an agency's BC/DR Plan shall be reviewed annually by the Office of the State CIO and recommendations shall be made for improvement, if necessary. |
| **Contingency Planning Team** | A team composed of representatives from the agency organizational areas with primary leadership responsibility to identify information technology risks and to determine what impact these risks have on business operations. |

| Role | Definition |
|---|---|
| **Third Party Service Providers** | Third party service providers are those vendors who provide and support contingency plans and capabilities. |

## CP-1 – Contingency Planning 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 Contingency Planning security controls at the organization, process and/or system level for all information assets / State data.

All State agencies must develop, adopt, and adhere to a formal, documented contingency planning procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The appropriate level of information technology business continuity management must be in place to sustain the operation of critical information technology services to support the continuity of vital business processes, also known as mission and business essential functions, and the timely delivery of critical automated business services to the State's citizens.

Appropriate planning and testing processes must be in place to ensure that, in the event of a significant business interruption, critical production environments can be recovered and sustained to meet State business requirements. To facilitate the effective recovery of systems and compliance with this policy, coordination is required between the Department of Information Technology (DIT), State, and Agency business units. This policy covers mainframe, distributed environments, and cloud-hosted environments, e.g., Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS).

The State has adopted the Contingency Planning security principles established in NIST SP 800-53, "Contingency Planning" control guidelines as the official policy for this security domain. The "CP" designator identified in each control represents the NIST-specified identifier for the Contingency Planning control family. The following subsections in this document outline the Contingency 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 Agency Management, or the Business Continuity Plan Administrator or Planner.

## CP-2 – Contingency Plan

The State's information assets must be available to authorized users when needed. Information technology risks must be managed appropriately as required in state and federal laws. A contingency plan/disaster recovery plan must be developed for the recovery of information assets for which the State is named as owner for all known threats to availability, including natural disasters, accidents, malicious destruction, failures, and denial of services. Management shall coordinate contingency plan development with organizational elements responsible for formally documenting the Business Continuity (BC) & Disaster Recovery (DR) Plan that covers all the agency's critical applications and includes procedures or references to procedures to be used for the recovery of systems that perform the agency's essential mission and critical business processes.

Application criticality has the following four categories (Definitions may be found in the Statewide Glossary of Information Technology Terms):

i. Noncritical
ii. Program Critical
iii. Department/Agency Critical
iv. Statewide Critical

Agencies with Statewide and Departmental Critical systems must provide disaster recovery capabilities to ensure timely recovery and restoration of service as part of their disaster recovery strategy. Agencies must coordinate contingency plan development and execution with agency divisions and groups responsible for related plans. Plans related to contingency plans for agency information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

Plans must include the following:

a. Be developed prior to implementation as part of the development life cycle for technology development or deployment by agency to address all production processing environments and assets.

b. Identify essential missions and business functions and associated contingency requirements.

c. Provide recovery time and recovery point objectives, restoration priorities; and estimate the following three downtime factors for consideration as a result of a disruptive event:

    i. Maximum Tolerable Downtime (MTD) - The amount of time vital business processes or mission essential functions can be disrupted without causing significant harm to the organization's mission.

ii. Recovery Time Objective (RTO) - The duration of time and a service level within which systems, applications, or functions must be restored after an outage to the predetermined Recovery Point Objective (RPO), for example, one business day (8 hours) or one day (24 hours).

iii. Recovery Point Objective (RPO) - The RPO represents the point in time, prior to a disruption or system outage, to which business processes or mission essential functions and supporting application data shall be recovered (given the most recent backup copy of the data) after an outage, e.g., the last completed transaction or the point immediately before the last backup commences.

d. Identify contingency roles, responsibilities, assigned individuals with contact information.

e. Address eventual, full information asset restoration without deterioration of the security measures originally planned and implemented.

f. Address the sharing of contingency information.

g. Be reviewed and approved by designated officials within the agency.

h. Be distributed to relevant system owners and stakeholders.

i. Coordinate contingency planning activities with incident handling activities.

j. Be revised to address changes to the organization, information asset, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

k. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into the contingency plan.

l. Protect the contingency plan from unauthorized disclosure and modification.

m. Address the protection of the health and safety of the employees of the State of North Carolina.

n. Address the protection of assets of the State and minimize financial, reputational, legal and/or regulatory exposure.

o. Create crisis teams and response plans for threats and incidents.

p. Require that employees are made aware of their roles and responsibilities in the BC/DR Plan and in plan execution through training and awareness programs.

q. Coordination with Contingency Plan Administrators and the Operations Team must occur for all potential outages that may result in a failover or recovery situation.

r. Be reviewed and submitted to the State CIO on an annual basis, and as otherwise requested by the State CIO.

s. Support the resumption of e vital business processes or mission essential functions within the agency-defined time period of contingency plan activation.

t. Define the time period for resumption of essential mission/business functions dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

u. Define within the contingency plan and Business Impact Analysis (BIA) the time period in which the system needs to be operational to support essential mission and business functions.

## CP-3 – Contingency Training

Personnel must be trained in their contingency roles and responsibilities with respect to the information assets. Training and awareness programs shall ensure that the organization understands the roles each individual within the organization in a disaster/or adverse situation. The contingency training content shall be reviewed and updated on an annual basis and following any defined events that necessitate change.

Contingency training shall be provided to information system users for the following conditions:

i. Prior to assuming a contingency role or responsibility,

ii. When required by information system changes,

iii. Annually thereafter.

## CP-4 – Contingency Plan Testing

Contingency plan testing must be coordinated with divisions and groups responsible for related plans. The following must be done:

a. Develop test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration procedures.

b. Test and/or exercise the contingency plan for the critical information assets annually, at a minimum, in order to determine the plan's effectiveness and the organization's readiness to execute the plan.

c. Develop a contingency plan exercise after action report.

d. Initiate corrective actions to ensure the procedures are adequate to restore/recover critical application processes. Document corrective actions in an After Action Report (AAR).

**Table 1 – Test Types**

| Test Type | Description |
|---|---|
| **Walk-Through** | A participatory session featuring an oral walk-through of the technology recovery plan and of the specific tasks documented within the plan. This exercise should |

| | |
|---|---|
| | confirm the plan's design and identify role and responsibility gaps or other weaknesses in the plan. This type of exercise can be used on alternating years between more complete testing for lower criticality systems. |
| **Table-Top** | A participatory session using example interruptions led by a facilitator to test the integrity of the disaster recovery plan as well as the readiness of the participating staff to respond to an adverse event. |
| **Stand-Alone** | Tests one or more specific components of a technology recovery plan in isolation from other components. Focuses on data restoration with network connectivity and is usually limited to a single platform or system. It may or may not include testing application interdependencies. |
| **Partial Integration** | Tests one or more specific components of a technology recovery plan. Includes testing data restoration with network connectivity and testing some interdependencies with applications and/or platforms. |
| **Full End-to-End** | Tests the technology recovery plan in a technology recovery testing environment without risk to the production environment, tests all components of the technology recovery plan and all functionality of an application. Includes testing transactions and testing all interdependencies with other applications and/or platforms. Tests shall be conducted at alternate sites or other recovery arrangements of the testing organization, personnel, equipment, facilities, and processes. |

## CP-5 – Contingency Plan Update

Withdrawn: Incorporated into CP-2.

## CP-6 – Alternate Storage Site

An alternate storage site must be established for systems that are defined as critical including necessary agreements to permit the storage and recovery of information asset backup information. The following must be done:

a. Ensure the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site.

b. Establish a site in a location that is separate from the primary facility to ensure that the risk of a disruption (e.g., natural disasters, structural failures, hostile cyber attacks) affecting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk.

c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by agencies based on agency assessments of risk. Explicit mitigation actions include, for example:

   i. Duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites;

   ii. Planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

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

## CP-7 – Alternate Processing Site

The following must be done for alternate processing:

a. Establish an alternate processing site including necessary agreements to permit the resumption of information asset operations for vital business processes or mission essential functions within defined recovery times and recovery points when the primary processing capabilities are unavailable. Alternate processing sites shall provide a Service Level Agreement (SLA) that contains priority-of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster. This may be in the form of a priority-of-service provision or through a provider with a sufficient network of facilities to ensure available capacity.

b. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the agency-defined time period for transfer/resumption.

c. Ensure that the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site.

d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

e. Determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern.

f. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

g. Outline and document explicit mitigation actions within the contingency plan.

h. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with agency availability requirements (including recovery time objectives). Priority-

of-service agreements refer to negotiated agreements with service providers that ensure that agencies receive priority treatment consistent with their availability requirements including defined RTO and RPO objectives as defined in the business impact analysis (BIA) and contingency plan.

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

## CP-8 – Telecommunications Services

The following must be done for telecommunication services:

a. Establish alternate telecommunications services with telecommunication service providers that provide communications transmission services to maintain a state of readiness or to respond to and manage any event or crisis.

b. Communications transmission services must include necessary agreements to permit the resumption of information asset operations for essential missions and business functions within defined recovery time and recovery points when the primary telecommunications capabilities are unavailable.

c. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agency availability requirements (including recovery time objectives).

d. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

e. Consider the potential process/function impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

f. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

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

## CP-9 – System Backup

a. Backups must be conducted of system documentation, such as operating system files and application software from organization managed laptops, workstations, servers, as well as security-and privacy-related documentation, and user level information, such as user level files stored on a shared network drive, at a frequency that is consistent with agency defined Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

b. The confidentiality and integrity of backup information must be protected.

## CP-9 (1) – Information System Backup | Testing for Reliability/Integrity

Backup information must be tested quarterly to verify media or cloud storage reliability, and information (data) integrity.

## CP-9 (8) – System Backup | Cryptographic Protection

Cryptographic mechanisms shall be implemented to prevent the unauthorized disclosure and modification of Agency-defined backup information.

## CP-10 – System Recovery and Reconstitution

The following must be done for system recovery and reconstitution:

a. Provide for the recovery and reconstitution of vital business processes/mission essential function(s), including transaction-based information systems, to a known state after a disruption, compromise, or failure within agency defined RTO and RPO objectives.

b. Applications categorized as Statewide and or Agency critical are recommended to have viable disaster recovery support, approval, budget in place, and be exercised according to policy.

c. Ensure plan activations are documented and recorded, and post-activation reviews are conducted to evaluate the effectiveness of the plan(s).

d. Update the plan(s) where necessary and provide a formal report to the State CIO within 30 days of post-activation review.

## CP-11 – Alternate Communication Protocols (Optional)

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

## CP-12 – Safe Mode (Optional)

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

## CP-13 – Alternative Security Mechanisms (Optional)

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.

| | Identification and Authentication Policy | Document No. SCIO-SEC-307 |
|---|---|---|

| Effective Date | Review Date | Version | Page No. |
|---|---|---|---|
| 01/29/2018 | 03/26/2025 | 4 | 1 of 12 |

## Scope

The Statewide Information Security Polices 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 (Agency CIO) to establish an agency wide 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 accessing or using IT resources are responsible for adhering to this policy and with any local Identification and Authentication requirements.

| Role | Definition |
|---|---|
| **Agency Management** | The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated agency officials at the senior leadership level are assigned the responsibility for the continued development, dissemination, implementation, operation and monitoring of the Identification and Authentication process. |
| **Agency Security Liaisons** | Agency Security liaisons are responsible for ensuring that adequate user identification and authentication controls are present in all agency computing environments including those managed by agencies or by third parties. |
| **Information System Owner** | The Information System Owner (SO) is responsible for ensuring that identification and authentication controls for the system are implemented in coordination with agencies, information owners, security system administration, and 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 (ISO)s 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. |
| **Covered Personnel** | Covered personnel are responsible for following the approved identification and authentication processes and the supporting controls. |
| **Third Parties** | Third party service providers with systems interconnected to the agency network are responsible for managing identification and authentication actions in accordance with this policy. |

## IA-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 Identification and Authentication security controls at the organization, process and/or system level for all information assets / State data. This policy provides requirements for the identification and authentication 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 has adopted the Identification and Authentication principles established in NIST SP 800-53, "Identification and Authentication" control guidelines as the official policy for this security domain. The "IA" designator identified in each control represents the NIST-specified identifier for the Identification and Authentication control family. The following subsections in this document outline the Identification and Authentication 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.

## IA-2 - Identification and Authentication Authorized Users

Information systems shall be configured to uniquely identify and authenticate users (or processes acting on behalf of users). Access to information systems is defined as either local access or network access. Local access is any access to information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network

access is access to information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (e.g., nonlocal access).

a. System Owners shall not allow the use of shared accounts (credentials used by more than one individual) within their system. The use of shared user accounts makes it difficult to uniquely identify individuals accessing an information system, as well as provide detailed accountability of user activity within an information system.

b. Identification and authentication mechanisms shall be implemented at the application level, as determined by a risk assessment, to provide increased security for the information system and the information processes. This shall be in addition to identifying and authenticating users at the information system level (e.g., when initially logging into a desktop, laptop, or mobile device).

c. Access to non-privileged accounts, privileged accounts, and all local accounts shall be authenticated with passwords, personal identification numbers (PINs), tokens, biometrics, or in the case of multifactor authentication (MFA), some combination thereof. **Note:** See IA–5 - Authenticator Management for definitions of privileged and non-privileged accounts.

## IA-2 (1) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts

MFA shall be implemented for access to privileged accounts.

## IA-2 (2) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-Privileged Accounts

a. MFA shall be implemented for remote network access with privileged and non-privileged accounts for information systems that receive, process, store, or transmit Restricted or Highly Restricted data.

b. MFA for remote access with privileged and non-privileged accounts shall be implemented such that one of the factors is provided by a device separate from the system gaining access. The purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system.

## IA-2 (8) - Identification and Authentication (Organizational Users) | Access to Accounts – Replay Resistant

Information systems shall implement replay-resistant authentication mechanisms for network access to privileged accounts, if technically configurable. Authentication processes resist replay

attacks if it is impractical for an attacker to replay previous authentication messages and thus achieve unauthorized access. Replay-resistant techniques include, for example, protocols that use challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators (one-time passwords).

## IA-2 (12) - Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Organizations shall accept and electronically verify Personal Identity Verification-(PIV) compliant credentials.

## IA-3 - Device Identification and Authentication

To protect State resources from vulnerabilities that can be introduced when users access the network with unmanaged devices, such as personal computing devices, all users accessing those resources shall adhere to required security configurations for devices, including required patches and updated anti-virus signature files on those devices.

a. Procedures that verify node authentication measures shall be developed.

b. Only approved procedures, mechanisms, or protocols shall be used for host or device authentication. Approved mechanisms and protocols include, but are not limited to, the following:

   i. Media Access Control (MAC) address filtering, which provides basic filtering based on Open Systems Interconnection (OSI) Layer 2 (Data Link Layer) address information.

   ii. Vendor-specific solutions which provide basic identification and authentication for devices in a wired network on a per-port basis.

   iii. Wi-Fi Protected Access 2 (WPA2) in combination with MAC filtering.

   iv. Institute of Electrical and Electronics Engineers (IEEE) 802.1x.

   v. Network Access Control (NAC) technology, which is most commonly built on the foundations of 802.1x.

c. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (“subnets”).

## IA–4 - Identifier Management

All information systems, to include cloud provided services, shall do the following:

a. Receive authorization from a designated agency representative (e.g., system administrator, technical lead, or system owner) to assign individual, group, role, service, or device identifiers.

b. Select and assign information system identifiers that uniquely identify an individual, group, role, service, or device. Assignment of individual, group, role, service, or device identifiers shall ensure that no two users or devices have the same identifier.

c. Prevent reuse of identifiers for seven (7) years.

d. Disable identifiers after ninety (90) days of inactivity, except as specifically exempted by agency management.

e. Delete or archive identifiers that have been disabled more than 365 days.

## IA-4 (5) Identifier Management | Identify User Status

Procedures shall be implemented to ensure that individual identifiers are managed by uniquely identifying each individual's credentials, such as employee, contractor, active, inactive, lock or disabled.

## IA–5 - Authenticator Management

Information system authentication requirements shall be managed. Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. The following shall be required:

a. Develop secure log-on procedures to be applied to all network components, operating systems, applications, and databases that implement a user identification and authentication mechanism. These procedures shall be designed to minimize the risk of unauthorized access.

b. Verify, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.

c. Establish initial authenticator content for authenticators issued by the organization.

d. Ensure that authenticators have sufficient strength of mechanism for their intended use.

e. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

f. Change default content of authenticators, for example, the default password immediately after system install.

g. Require individuals to take, and have devices implement, specific security safeguards to protect authenticators from unauthorized disclosure and modification.

h. Change authenticators for group/role accounts when membership to those accounts change.

i. Information systems shall display a message to users before or while they are prompted for their user identification and authentication credentials that warns against unauthorized or unlawful use. Refer to the Access Control policy AC-8 - System Use Notification for the standard State approved banner.

j. The log-on process should not be validated until all log-on data is input. Failing the process as each input field is completed will provide an attacker with information to further the attack.

k. Only generic "log-on failed" messages should be displayed if the user does not complete the log-on process successfully. Do not identify in the message whether the user identification, password, or other information is incorrect.

l. Systems shall be configured to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds the established limit, the configuration shall either force a time delay before further log-on attempts are allowed or shall disable the user account such that it can only be reactivated by a system or security administrator or an authorized service desk staff member.

m. For systems that store, transmit, or process FTI, the agency shall password-protect the system initialization (boot) settings.

n. All newly assigned passwords shall be changed the first time a user logs into the information system.

o. Where technically configurable, passwords shall be at least fourteen (14) characters long for access to all systems and applications.

p. Passwords shall consist of at least one (1) numeric, at least one (1) uppercase, at least one (1) lowercase letter, and at least one (1) special character.

q. Passwords shall not contain number or character substitutes to create dictionary words (e.g., d33psl33p for deepsleep).

r. Account passwords shall not traverse the network or be stored in clear text. All passwords stored shall be encrypted using FIPS-140-2 encryption.

s. Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption.

t. Information systems may allow the use of a temporary password for system logons if the temporary password is immediately changed to a permanent password upon the next logon attempt.

u. Passwords shall be different from all other accounts held by that user.

v. Agencies may use approved password management tools. Approved password managers must be installed and managed locally on the user's machine (not offsite or in the "cloud"), must

securely store passwords with a master key or key file, and must encrypt the password list with FIPS 140-2 encryption (e.g., AES 256).

In addition, agencies shall not use freeware solutions but rather purchase enterprise solutions. Also, agencies must create Standard Operating Procedures (SOPs) for the operations and management of such tools.

w. Passwords shall not be revealed to anyone, including supervisors, help desk personnel, security administrators, family members or co-workers.

x. Users shall enter passwords manually for each application or system, except for simplified/single sign-on systems that have been approved by the State CIO.

y. Passwords shall be changed whenever there is the suspicion or likelihood that the password or system is compromised.

z. The identity of an end user shall be validated when a password reset is requested. Initial passwords and subsequent password resets shall utilize a unique password for each user account.

aa. Passwords that are at least fourteen (14) characters long shall not be reused until five (5) additional passwords have been created. If passwords are less than fourteen (14) characters long, they must not be reused until twenty-four (24) additional passwords have been created.

bb. Passwords shall not have a minimum lifetime when used as an initial password or during a reset where a temporary password is provided. Use of this type of password shall be configured to require an immediate change on first use.

## Password Management Standards – Non-Privileged Accounts

A non-privileged account is generally defined as a standard user account that does not have elevated privileges, such as administrator access to a system. For instance, non-privileged accounts cannot make configuration changes to an information system or change the security posture of a system. Information systems that use password-based authentication shall do the following:

a. Passwords shall have a minimum lifetime of one (1) day and a maximum lifetime of one year with MFA and one hundred eighty (180) days without MFA. For directory-based accounts, where the account can be used multiple places, MFA must be enforced for all instances to qualify for “with MFA”.

b. While the State is transitioning to the new standard stated above, passwords less than fourteen (14) characters long for non-privileged accounts shall have a maximum lifetime of ninety (90) days.

c. Passwords for citizens and business users are recommended to be changed at least annually.

## Password Management Standards – Privileged Accounts

A privileged account is generally defined as a system administrator account. Privileged accounts have elevated permissions that allow them to do certain tasks a non-privileged user account cannot. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router management.

a. Privileged accounts are generally used for performing administrative functions, such as configuration changes, system/software upgrade, patch installations, and/or developing software.

b. Privileged accounts shall have passwords with a minimum lifetime of one (1) day and a maximum lifetime of one hundred eighty (180) days with MFA and ninety (90) days without MFA. For directory-based accounts, where the account can be used multiple places, MFA must be enforced for all instances to qualify for "with MFA".

d. While the State is transitioning to the new password lifetime standard stated above, passwords less than fourteen (14) characters long for privileged accounts shall have a maximum lifetime of thirty (30) days.

## Password Management Standards—Service Accounts

A service account is a non-interactive account created by system administrators for automated use by an application, operating system, or network device for their business purpose. Service accounts shall be managed by the following:

a. Service accounts shall only be granted the minimum level of access required to run a process.

b. Service accounts must be dedicated solely to their business purpose and not shared by an end user.

c. Service accounts shall be separate from privileged and non-privileged accounts.

d. All service accounts must have appropriate logging as specified by the agency of account activity. The application/device owner must audit the service account usage semi-annually, at a minimum.

e. Whenever technically configurable, service account passwords must have change intervals appropriate to the level of risk posed by a potential compromise of the system. At a minimum, change intervals shall not exceed 364 days (1 year).

f. A service account password must be changed immediately after any potential compromise or any individual who knows the password leaves the organization or changes roles within the organization.

g. In the special case where an application or system is *specifically designed* for service accounts to use 'non-expiring' passwords to complete their business purpose, these accounts must be preapproved by agency management and the agency's security liaison. Agency approved controls, policies, and procedures must be in place to closely monitor and mitigate the risk of non-expiring passwords.

## IA-5 (1) Authenticator Management | Password-based authentication

The following shall be done for password-based authentication:

a. Utilize a list of commonly used, expected, or compromised passwords that is regularly updated. The list should be reviewed at an organization defined frequency.

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the composition and complexity rules defined in IA (5).

## IA-5 (6) Authenticator Management | Protection of Authenticators

Authenticators shall be protected commensurate with the security category of the information to which use of the authenticator permits access.

## IA-6 - Authenticator Feedback

All information systems including those operated on behalf of the agencies shall ensure the following:

i. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

j. Mask passwords upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.

## IA-7 - Cryptographic Module Authentication

a. Mechanisms shall be implemented for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

b. Validation provides assurance that when an organization implements cryptography, the encryption functions have been examined in detail and will operate as intended.

c. All encrypted electronic transmissions must be encrypted using FIPS 140-2 validated cryptographic modules. NIST maintains a list of validated cryptographic modules on its website at http://csrc.nist.gov/.

## IA-8 – Identification and Authentication (Non-Agency Users)

This control typically applies to information systems that are accessible to the general public, for example, public-facing websites. The following shall be done for all non-agency users accessing information systems, including those operated on behalf of the agencies.

a. Approved third-party credentials must meet or exceed the set of minimum state and federal technical, security, privacy, and agency maturity requirements.

b. Information systems shall be configured to uniquely identify and authenticate non-agency users or processes acting on behalf of non-agency users.

c. Information systems shall uniquely identify and authenticate non-agency users for all access other than those explicitly identified and documented as exceptions in the Access Control Policy SCIO-SEC-301 regarding permitted actions without identification and authentication.

## IA-9 - Service Identification and Authentication (Optional)

This control is optional for Low and Moderate risk information systems.

## IA-10 - Adaptive Identification and Authentication (Optional)

This control is optional for Low and Moderate risk information systems.

## IA-11 - Re-Authentication

Organizations may require users to re-authenticate during the following circumstances / situations:

a. When an account changes and necessities re-authentication,

b. When a privileged function occurs,
c. When the user's role changes,
d. After an agency defined fixed period of time.

## IA-12 Identity Proofing

Organizations shall ensure the following:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

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

## IA-12 (2) Identity Proofing |Identity Evidence

Evidence of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the registration authority. A registration authority refers to the department, team and/or role that owns the process of validation and verification of an identity. If required, this authority could use external sources/services for completion of the validation and verification of the individual's identity.

## IA-12 (3) Identity Proofing | Identity Evidence Validation and Verification

The presented identity evidence shall be validated and verified through agency defined methods of validation and verification. Depending on the type of position and the risk of the job role/position, defined methods include the validation and verification of the following documentation:

a. ID card issued by Federal, state, or local government

b. US Passport

c. Birth Certificate

d. Permanent Resident Card

e. School ID card with a photograph

## IA-12 (5) Identity Proofing | Address Confirmation

A registration code or a notice of proofing must be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

## 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.

## 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 who utilize State of NC IT resources are responsible for adhering to this policy and with any local Incident Response requirements based on their assigned responsibilities defined below.

| Role | Definition |
|---|---|
| **Agency Management** | The State Chief Information Officer (SCIO), Agency Chief Information Officer (CIO), Chief Information Security Officer (CISO), or other designated agency officials at the senior leadership level are assigned the responsibility for the continued development, dissemination, implementation, operation and monitoring of the Incident Response program. |
| **Incident Response Officer** | The Incident Response Officer (IRO) is a senior or executive level individual such as the CISO, CIO or Agency Security Liaison who is accountable for the actions of the IR team and the IR function. |
| **Incident Response Manager (IRM)** | Reporting to the IRO, the Incident Response Manager (IRM) is responsible for leading the efforts of the Incident Response Team (IRT) and coordinates activities between all of its respective groups. The IRM is responsible for activating the IRT team and managing all parts of the IR process, from discovery, assessment, remediation and finally resolution. |

| | |
|---|---|
| | This role typically resides with the Enterprise Security and Risk Management Office (ESRMO). |
| **Incident Response Team (IRT)** | Reporting to the IRM, the IRT is comprised of representatives from IT, Security, Application Support and other business areas. Members of a IRT are responsible for providing accelerated problem notification, containment, and recovery services in the event of computer security related emergencies, such as virus infections, unauthorized access, or other events that may compromise production systems or information. All information security incidents must be handled with the involvement and cooperation of NCDIT. |
| **Local Incident Response Coordinator** | Reporting to the IRM, the Local Incident Response Coordinator (LIRC) is the Agency Security Liaison. This person is recognized as the local IR leader and is able to direct efforts of the local incident responders during an incident and provide status updates to the IRM |
| **Incident Responders** | Reporting to the IRM or the LIRC during an incident depending on their location, these technical experts are identified and called upon to assist in the remediation and resolution of a given incident. |
| **Covered Personnel** | Covered personnel have the responsibility to report information technology security incidents, software errors or weaknesses to agency management in accordance with statewide information security standards and agency standards, policies, and procedures. The notification shall be made as soon as possible after the weakness is discovered. |
| **Third Parties** | Third party service providers must provide Incident Response 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. Incident Response plans are subject to periodic review of incident response controls by the State. |

# IR-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 Incident Response (IR) security controls at the organization, process and/or system level for all information assets / State data. This policy provides requirements for the incident response process which is required to assure that information systems are designed and configured using controls sufficient to safeguard the State's information systems. The requirements described in this Incident Response policy are designed to help agencies respond to and minimize the impact of cybersecurity incidents of information systems and data of which the State is considered the owner.

The State has adopted the Incident Response principles established in NIST SP 800-53, "Incident Response" control guidelines as the official policy for this security domain. The "IR" designator identified in each control represents the NIST-specified identifier for the Incident Response control family. The following subsections in this document outline the Incident Response 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.

## IR-2 – Incident Response Plan Training

Personnel with access to the State network must be trained in their incident response roles. Incident response training must be provided to information system users that is consistent with assigned roles and responsibilities. Organizations shall do the following:

a. Provide training prior to assuming an incident response role or responsibility, or acquiring access, or when required by information system changes, and annually thereafter.

b. Provide additional or supplemental IR training when information system changes occur.

c. Include user incident response training regarding the identification and reporting of suspicious activities, both from external and internal sources.

d. Review and update IR content on a regular basis and/or following agency defined events including but not limited to assessment or audit findings or changes to guidelines. Maintain a comprehensive record of all IR related training. The electronic log shall include names of participants, information system name(s), type of training, and date of completion. Log entries shall be maintained by the Agency Security Liaison or designee.

## IR-3 – Incident Response Plan Testing

All incident response personnel and service providers must perform the following testing:

a. Identify essential missions and business functions and associated incident response requirements.

b. Organizations must perform tabletop exercises using scenarios that include a breach of Restricted or Highly Restricted data and should test the organization's incident response policies and procedures.

c. A subset of all employees and contractors with access to Restricted or Highly Restricted data must be included in tabletop exercises.

d. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

e. Organizations entrusted with Restricted or Highly Restricted data must test the incident response capability at least annually.

f. For systems that store, process, or transmit federal tax information (FTI), see Section 1.8.4, Incident Response Procedures in IRS 1075, for specific instructions on incident response requirements.

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

## IR-3 (2) – Incident Response Plan Testing | Coordination with Related Plans

Agencies shall coordinate incident response testing with agency elements responsible for related plans. Agency plans related to incident response testing include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans (COOP), Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

## IR-4 – Incident Handling

Organizations shall protect technology resources by conducting proper investigations:

a. The IRM, acting on behalf of the SCIO, shall evaluate the proper response to all information technology security incidents reported to the agency.

b. The IRM shall work with agencies to decide what resources, including law enforcement, are required to best respond to and mitigate the incident.

c. After the initial reporting and/or notification, agency management shall review and reassess the level of impact that the incident created.

d. The IRM shall coordinate incident handling activities with contingency planning activities.

e. Organizations shall ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. This will help ensure consistency in the incident handling procedure put in place in terms of steps/logistics, communications, coordination, and planning functions needed to resolve an incident in a structured and efficient manner. This is best achieved by following NIST guidelines such as the following:

i. NIST SP 800-83, Guide to Malware Prevention and Incident Handling for Desktops and Laptops, Revision 1;

ii. NIST SP 800-61 Computer Security Incident Handling Guide, Revision 2 (Section 3);

iii. NIST SP 800-92 Guide to Information Security Log Management.

f. An investigation into an information technology security incident must identify its cause, if possible, and appraise its impact on systems and data. The extent of damage must be determined and course of action planned and communicated to the appropriate parties.

g. Organizations shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (i.e., hardware or software failure).

h. If any suspicious activities are detected, responsible personnel within the affected agency shall be notified to ensure that proper action is taken.

i. Agencies shall establish controls to protect data integrity and confidentiality during investigations of information technology security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure fraudulent activities requiring collusion do not occur.

j. Evidence of or relating to an information technology security breach shall be collected and preserved in a manner that is in accordance with State and federal requirements.

k. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident.

l. Any system, network, or security administrator who observes an intruder on the State network or system shall take appropriate action to terminate the intruder's access. (Intruder can mean a hacker, botnet, malware, etc.)

m. In the event of an active incident, agency management has the authority to decide whether to continue collecting evidence or to restrict physical and logical access to the system involved in the incident. **Note**: It may be necessary to isolate from the network until the extent of the damage can be assessed.

n. When dealing with a suspected incident, the following shall be done:

i. Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved.

ii. Make copies of all audit trail information such as system logs, network connections (including IP addresses, TCP/UDP ports, length, and number), super user history files, etc.

iii. Take steps to preserve and secure the trail of evidence.

o. The Agency's CIO or his/her designee will determine if other agencies, departments, or personnel need to become involved in resolution of the incident. Agencies shall consider coordinating IR activities with external organizations, such as the OSA, OSHR, SBI, or the FBI.

p. All personnel directly involved with incident handling shall have signed a Non-Disclosure Agreement (NDA).

q. Incident details shall be discussed only on a need-to-know basis with authorized personnel.

r. When responding to a malware threat, the following tasks shall be performed:

   i. Verify threats to rule out the possibility of a hoax before notifying others

   ii. Identify personnel responsible for mitigation of malware threats

   iii. Have internal escalation procedures and severity levels

   iv. Have processes to identify, contain, eradicate, and recover from malware events

   v. Have a contact list of antivirus software vendors

s. The following may be utilized for guidance regarding incident handling:

   i. NIST SP 800-36, Guide to Selecting Information Technology Security Products;

   ii. NIST SP 800-61, Computer Security Incident Handling Guide, Revision 2;

   iii. NIST SP 800-83, Guide to Malware Prevention and Incident Handling for Desktops and Laptops, Revision 1;

   iv. NIST SP 800-86, Guide for Integrating Forensic Techniques into Incident Response;

   v. NIST SP 800-92, Guide to Information Security Log Management;

   vi. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS);

   vii. NIST SP 800-101, Guidelines on Mobile Device Forensics, Revision 1; and

   viii. Other appropriate guidance, as necessary.

t. Organizations shall activate and implement a security incident handling capability that is consistent with the IR plan; during all stages of the NIST incident response life cycle (See Figure 1), including the following:

   i. Preparation

   ii. Detection and Analysis

   iii. Containment, Eradication, and Recovery

   iv. Post-Incident Activities

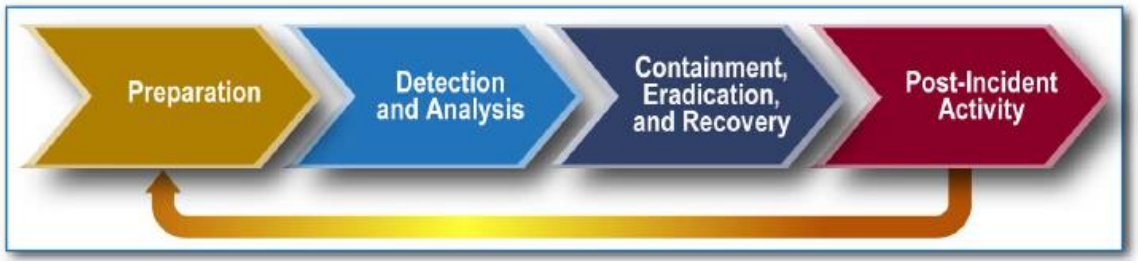


Figure 1

u. The integrity of information systems incident investigations shall be ensured by having the records of such investigations audited by qualified individuals as determined by agency management.

v. Records of information security breaches and the remedies used for resolution shall be maintained as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned.

w. The agency/department IT manager and/or incident response coordinator shall determine the criticality of an incident (see IR-6 for severity levels).

x. Lessons learned from incident handling activities shall be incorporated into incident response procedures, training, and testing/exercises, and implements the resulting changes.

y. Organizations shall create processes to provide information for the enhancement of information security awareness programs and incident response programs.

## IR -4 (1) – Incident Handling | Automated Incident Handling Process

Automated processes shall be enacted for the purpose of correlating security events, e.g., Security Information and Event Management (SIEM) technology.

## IR-5 – Incident Monitoring

Maintaining records about each information system incident, the status of the incident, and other pertinent information is necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

a. Information system security incidents that potentially affect the confidentiality of all other Restricted and Highly Restricted data shall be tracked and documented.

b. If the incident is rated a severity 3 or higher (see IR-6 for severity levels), subsequent reports to agency management shall be provided.

c. The release of confidential security information during a security incident or investigation shall be monitored and controlled to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel or human resources.

d. A follow-up report shall be submitted to agency management upon resolution by those directly involved in addressing the incident and contain the following:

   i. Point of contact

   ii. Affected systems and locations

   iii. System description, including hardware, operating system, and application software

   iv. Type of information processed

   v. Incident description

   vi. Incident resolution status

   vii. Damage assessment, including any data loss or corruption

   viii. Organizations contacted

   ix. Corrective actions taken

   x. Lessons Learned

## IR-6 – Incident Reporting

Security incidents, for example, suspicious events (e.g., insider threat), software errors or weaknesses, system vulnerabilities associated with security incidents (e.g., Ransomware), and lost or stolen State computer equipment, shall be reported *immediately* to the agency management.

a. Agencies and vendors of the State shall ensure all suspected security incidents or security breaches are reported to the ESRMO within twenty-four (24) hours of incident confirmation, as required by NC general statute. Incidents shall be reported to the ESRMO by one of the following methods:

   i. Contact DIT Customer Support Center 800-722-3946

   ii. Use the incident reporting website https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form.

iii. Contact a member of the DIT Threat Management staff directly by phone or email dit.threatmanagement@nc.gov.

b. Contracts involving the storage and/or processing of State data shall identify the vendor's security point of contact (PoC).

c. For incidents involving FTI, agencies shall contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards *immediately* but no later than 24 hours after identification of a possible issue involving FTI. Refer to IRS 1075 Section 1.8, Reporting Improper Inspections or Disclosures, for more information on incident reporting requirements.

d. For reporting security incidents to outside authorities, agencies shall do the following:

i. Agencies shall coordinate with ESRMO in accordance with the State's Incident Response Plan, applicable state laws, procedures, and agreements that require reporting to the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor. All security incidents shall be reported to the ESRMO when reported to an outside entity.

ii. Organizations shall notify the Social Security Administration (SSA) Regional Office and their SSA Systems Security Contact within one (1) hour of suspecting loss if a privacy or security incident involves the unauthorized disclosure of Social Security data. If the security incident is related to the State Transmission/Transfer Component (STC) and the agency is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the STC must report the incident by contacting SSA's National Network Service Center (NNSC).

iii. If a security incident involves the possible breach of FTI, the agency must contact the appropriate special agent-in-charge, the Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards immediately, but no later than twenty-four (24) hours after identification.

iv. Organizations shall notify consumers in the event of a security breach resulting in the unauthorized release of unencrypted or un-redacted records or data containing personal information with corresponding names. **Note**: The acquisition of encrypted data is only a breach if a confidential process or key needed to unlock the data is also breached, or if the data is encrypted by an unauthorized or malicious process, such as ransomware.

v. The Agency CIO and/or his/her designee shall manage the dissemination of incident information to other participants, for example law enforcement or the press. Public release of information concerning a security incident shall be coordinated through the Agency's CIO, the Incident Response Team (IRT), and the agency's Public Information Officer (PIO).

e. Information recorded about information technology security breaches shall cover the following at a minimum:

i. Identify the current level of impact on agency functions or services (Functional Impact).

ii. Identify the type of information lost, compromised, or corrupted (Information Impact).

iii. Estimate the scope of time and resources needed to recover from the incident (Recoverability).

iv. Identify when the activity was first detected and when corrective actions were implemented.

v. Identify the number of systems, records, and users impacted.

vi. Identify the network location of the observed activity.

vii. Identify point of contact information for additional follow-up.

viii. Identify the attack vector(s) that led to the incident.

ix. The method of breach detection and incident response actions

x. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.

xi. Provide any mitigation activities undertaken in response to the incident.

## Incident Severity Levels

The Incident Response Manager (IRM) is responsible for initially assessing an incident's impact, and assigning a severity to the incident. This initial severity assignment dictates the level of response to the incident. As response to the incident progresses, it may be determined that the incident is more (or less) severe than originally realized, and a new severity level assigned. Security incidents are divided into five levels of severity based on their potential to negatively impact North Carolina agency operations, finances, and/or reputation. The characteristics in the table below should be used as baseline severity levels and may include additional threats categories.

| Incident Severity | Incident Characteristics |
|---|---|

| | |
|---|---|
| 5<br>**GENERAL ATTACK(S)**<br>**SEVERE** | • Potential for or actual loss of lives or significant impact on the health or economic security of the state<br>• Significant risk of negative financial or public relations impact<br>• Loss of critical supervisory control and data acquisition (SCADA) systems<br>• Successful penetration or denial-of-service attack(s) detected with significant impact on North Carolina state network operations:<br>○ Very successful, difficult to control or counteract<br>○ Large number of systems compromised<br>○ Significant loss of confidential data<br>○ Complete network failures<br>○ Mission-critical system or application failures<br>○ Compromise or loss of administrative controls of critical system |
| 4<br>**LIMITED ATTACK(S)**<br>**HIGH** | • Low risk of negative financial or public relations impact<br>• Widespread instances of a computer virus or worm that cannot be handled by deployed anti-virus software<br>• A critical vulnerability is discovered but no exploits are reported<br>A critical vulnerability is being exploited but there has been no significant impact<br>• Penetration or denial-of-service attack(s) detected with limited impact on State network operations:<br>○ There are credible warnings of increased probes or scans<br>○ Minimally successful, easy to control or counteract<br>○ Small number of systems compromised<br>○ Little or no loss of confidential data<br>○ No loss of mission-critical systems or applications<br>○ A compromise of non-critical system(s) did not result in loss of data |
| 3<br>**SPECIFIC RISK OF ATTACK**<br>**ELEVATED** | • An exploit for a critical vulnerability exists that has the potential for significant damage<br>• A critical vulnerability is being exploited and there has been a moderate impact<br>• There is a compromise of a secure or critical system(s) containing sensitive information<br>• There is a compromise of a critical system(s) containing non-sensitive information, if appropriate<br>• Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software<br>• Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software<br>• There is a distributed denial of service attack.<br>• Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance |

| | |
|---|---|
| 2<br>**INCREASED RISK OF ATTACK**<br>**GUARDED** | • A critical vulnerability is discovered but no exploits are reported.<br>• A critical vulnerability is being exploited but there has been no significant impact.<br>• A new virus is discovered with the potential to spread quickly.<br>• There are credible warnings of increased probes or scans.<br>• A compromise of non-critical system(s) did not result in loss of data.<br>• Small numbers of system probes, scans, and similar activities detected on internal systems<br>• External penetration or denial of service attack(s) attempted with no impact to State network operations<br>• Intelligence received concerning threats to which State NCDIT systems may be vulnerable |
| 1<br>**LOW** | • Small numbers of system probes, scans, and similar activities detected on internal and external systems<br>• Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software<br>• Unsubstantiated or inconsequential event |

## IR-6 (1) Incident Reporting | Automated Reporting

Automated processes shall be enacted for the purpose of reporting incidents e.g., Security Information and Event Management (SIEM) technology.

## IR-6 (3) Incident Reporting | Supply Chain Coordination

A process shall be ensured to provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident. Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel.

## IR-7 - Incident Response Assistance

The ESRMO shall provide incident response support that offers advice and assistance to users of State and agency managed information systems for the handling and reporting of security incidents. These resources may include digital forensic services, vulnerability assessments, and incident response capability. Agencies and service providers of the State shall establish and maintain a cooperative relationship between its IR capability and the State's IR capability, and other external, key providers of information systems.

## IR-7 (1) - Incident Response Assistance – Automation Support for Availability of Information and Support

The availability of incident response information and support shall be increased with the use of automated mechanisms. Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. Examples of automated mechanisms to provide IR information and support include the following:

- Ticketing system for help desk
- Distribution lists
- Automated answering

## IR-8 - Incident Response Plan

Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. All Incident Response plans must include the following requirements:

a. Provides the organization with a roadmap for implementing its incident response capability,

b. Describes the structure and organization of the incident response capability,

c. Provides a high-level approach for how the incident response capability fits into the overall agency,

d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions,

e. Defines reportable incidents,

f. Provides steps to be taken within the security incident response plan during and after cyberattacks,

g. Provides metrics for measuring the incident response capability within the organization by incident response management function:

   i. Common organizational interfaces: e.g., communications, work coordination

   ii. Protect: e.g., risk assessment, malware protection, vulnerability management

   iii. Detect: e.g., network security monitoring and alerting

   iv. Respond: e.g., incident reporting, incident response, incident analysis

   v. Sustain: e.g., MOUs and contracts, program management, security administration

h. Defines the resources and management support needed to effectively maintain and mature an incident response capability,

i. Addresses the sharing of incident information, with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving Restricted or Highly Restricted data (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

j. Be reviewed and approved by designated State or agency officials annually, at a minimum,

k. Explicitly designate the responsibility for incident response to an agency defined role/personnel.

l. Be revised as needed to address system/agency changes or problems encountered during plan implementation, execution, or testing,

m. Incident response plan changes must be communicated to identified State and agency officials,

n. Incident response plans must be distributed to State and agency identified incident response personnel,

o. Protect the incident response plan from unauthorized disclosure and modification.

## IR-9 - Incident Spillage Response (Optional Control)

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

For incident spillage involving FTI, agencies shall refer to IRS 1075 for additional guidance.

## IR-10 - Integrated Information Security Analysis Team (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.

## 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 maintenance requirements.

| Role | Definition |
|---|---|
| **Chief Information Security Officer** | 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 the continued development, dissemination, implementation, operation, support and promotion of the information system security maintenance program throughout the agencies. |
| **Agency Security Liaison** | The Security liaison is responsible for ensuring that assigned information systems and supporting infrastructure are maintained in compliance with State requirements by collaborating with organizational entities.<br>Liaisons are responsible for maintaining the appropriate operational security posture for agency controlled information system or program. |
| **Information System Owner** | The Information System Owner (SO) is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |

| | |
|---|---|
| **Third Parties** | Third party service providers with systems interconnected to the State network are responsible for maintaining their systems in accordance with this policy. |

## MA-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 Maintenance security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the Maintenance security principles established in NIST SP 800-53, "Maintenance" control guidelines as the official policy for this security domain. The "MA" designator identified in each section represents the NIST-specified identifier for the Maintenance control family. The following subsections in this document outline the Maintenance 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.

To maintain the highest level of system availability and protect the agency's infrastructure, maintenance operations must be performed at predetermined, authorized times or on an approved, as-needed basis.

a. Maintenance policies and procedures must be developed and maintained to facilitate the implementation of the information system security maintenance requirements and associated system information system security maintenance controls.

b. The current information system security maintenance requirements and procedures must be reviewed and updated at least annually or when significant changes occur.

## MA-2 – Controlled Maintenance

The following shall be done:

a. Establish normal change controls and maintenance cycles for resources.

b. Perform maintenance of operating systems in accordance with approved information technology security requirements.

c. Consider the following issues when supporting operating systems:

i. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities.

ii. Periodic maintenance improves the performance of operating systems (e.g., hard drive defragmentation).

iii. The operating systems on servers, minicomputers and mainframes usually require daily maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded.

d. Ensure that system administrators shall apply all current maintenance and security vulnerability patches and that only essential application services and ports are enabled and opened in system and network firewalls.

e. Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure the following:

i. Maintenance tasks continue to function as expected.

ii. Operating systems continue to operate within accepted thresholds.

iii. System security is not being compromised by maintenance tasks.

iv. Maintenance tasks do not adversely affect computer capacity or performance.

f. Ensure that software faults or bugs are formally recorded and reported to those responsible for software support and maintenance.

g. Restrict physical access to systems (e.g., by locating them in protected data center or dedicated, locked storage rooms).

h. Apply a comprehensive set of management tools (e.g., maintenance utilities, remote support, enterprise management tools and backup software) to keep them up to date (e.g., by applying approved change management and patch management processes).

i. Monitor information systems (e.g., using Simple Network Management Protocol (SNMP)) so that events such as hardware failure and attacks against them can be detected and responded to effectively. For public and private networks, management software tools that communicate with devices shall use SNMP version 3 for network management.

j. Review maintenance records on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed on the server (e.g., by inspecting logs).

k. Provide or arrange maintenance support for all equipment that is owned, leased, or licensed by the agency.

l. Arrange support services through appropriate maintenance agreements or with qualified technical support staff.

m. When maintenance support is provided by a third party, nondisclosure agreements (NDAs) shall be signed by authorized representatives of the third party before any maintenance support is performed.

n. Schedule, perform, document, and review records of information system security maintenance, repairs, and replacement on information system components in accordance with manufacturer or vendor specifications and organizational requirements.

o. Maintain records of all maintenance activities.

p. Approve and monitor all maintenance activities to include routine scheduled information system security maintenance and repairs, whether the system or system component is serviced onsite, remotely, or moved to another location.

q. Ensure removal of the information system or any of its components from the facility for maintenance, repair, or replacement is first approved by an appropriate official.

r. Sanitize equipment to remove all Restricted or Highly Restricted information from associated media, following proper procedure, when the information system or any of its components require offsite information system security maintenance, repairs, replacement.

s. Verify proper functionality of all potentially impacted security controls after information system security maintenance or replacement is performed.

t. Restrict the use of root/administrator privilege to only when required to perform duties.

u. Establish normal change controls and maintenance cycles for resources.

v. Maintain information system security maintenance records for the information system to include the following:

   i. Date and time of information system security maintenance

   ii. Name of the individual performing the information system security maintenance

   iii. Name of escort, if necessary

   iv. Description of the information system security maintenance performed; and

   v. List of equipment removed or replaced (including identification numbers, if applicable).

w. Employ automated mechanisms to schedule and conduct the information system security maintenance as required, to create up-to-date, accurate, complete, and available records of all information system security maintenance actions. This requirement is only applicable for information systems with a “HIGH” security categorization based on its impact on critical business processes and the sensitivity of the data contained within the system. The

categorization of "HIGH," "MEDIUM or "LOW" is defined in the Statewide Data Classification and Handling Policy: https://it.nc.gov/documents/statewide-data-classification-handling-policy

## MA-3 – Maintenance Tools

The following are required for the use of information system security maintenance tools:

a. Approve, control, and monitor the use of information system security maintenance tools and maintain these tools on an ongoing basis.

b. Review previously approved system security maintenance tools.

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

## MA-3 (1) – Maintenance Tools | Inspect Tools

Inspect all maintenance tools carried into a facility by information system security personnel for unauthorized modifications or malicious code and handle the incident consistent with State and agency incident response policies and procedures.

## MA-3 (2) – Maintenance Tools | Inspect Media

Check all media containing diagnostic and test programs for malicious code before they are used in the information system. If, upon inspection of media containing maintenance diagnostic and test programs, agencies determine that the media contains malicious code, the incident is handled consistent with State and agency incident handling policies and procedures.

## MA-3 (3) – Maintenance Tools | Prevent Unauthorized Removal

Prevent the unauthorized removal of maintenance equipment which can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers as follows:

a. Verify that there is no State or agency data contained on the equipment;

b. Sanitize or destroy the equipment;

c. Retain the equipment within the facility; or

d. Release to the State Office of Surplus Property or a third-party disposal facility upon management approval explicitly authorizing the removal of the equipment from the facility.

## MA-4 - Nonlocal Maintenance

Nonlocal (remote access) maintenance and diagnostic activities of information systems is allowed only as consistent with State policy and documented in the security plan for the information system, and shall be conducted by individuals through either internal or external networks with the following requirements:

a. Approve and monitor nonlocal maintenance and diagnostic activities.

b. Employ multi-factor authentication (MFA) that combines at least two mutually independent factors such as challenge / response answers, biometrics, and tokens, for nonlocal maintenance and diagnostic sessions to protect the integrity and confidentiality of communications.

c. Maintain records for nonlocal maintenance and diagnostic activities.

d. Terminate session and network connections when nonlocal maintenance is completed.

## MA–5 - Maintenance Personnel

All individuals performing hardware or software maintenance on State or agency information systems shall have the proper access authorizations needed to connect to networks to perform maintenance activities.

a. Establish a process for information system security maintenance personnel authorization and maintain a current list of authorized information system security maintenance organizations or personnel.

b. Verify that non-escorted personnel performing information system security maintenance locally or remotely have appropriate access authorizations to the information system allowing access to State data. Inappropriate access would result in a compromise of confidentiality, integrity, or availability.

c. Designate personnel with required access authorizations and technical competence to supervise the information system security maintenance activities of personnel who do not possess the required access authorizations.

## MA-6 - Timely Maintenance

Preventative information system security maintenance support shall be performed for the purpose of maintaining equipment and facilities in satisfactory operating conditions.

a. Predictive maintenance, or condition-based maintenance shall be performed by conducting periodic or continuous (online) equipment condition monitoring.

b. Where technically configurable, automated mechanisms should be used to transfer predictive maintenance data to a computerized maintenance management system.

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

## Support for Operating Systems

Operating systems used to run the production environment shall be regularly monitored for security risks and maintained in approved secure configurations to support business operations. The following issues should be considered when supporting operating systems:

a. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities.

b. Periodic maintenance improves the performance of operating systems (e.g., hard drive defragmentation).

c. The operating systems on servers, minicomputers and mainframes usually require daily maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded.

d. Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure that the following:

   i. Maintenance tasks continue to function as expected.

   ii. Operating systems continue to operate within accepted thresholds.

   iii. System security is not being compromised by maintenance tasks.

   iv. Maintenance tasks do not adversely affect computer capacity or performance.

## Operating System Software Upgrades

Operating system (OS) upgrades shall be carefully planned, executed, and documented as a project. The following steps shall be performed before commencement of an upgrade project:

a. Document that system security controls will remain effective or will be modified to appropriately respond to the OS upgrade.

b. Locate change control processes and procedures.

c. Document agreement of technical staff and management to acceptance criteria.

d. Document that qualified personnel have certified the upgrade and that it has passed user acceptance testing.

e. Establish a rollback plan in the event the upgrade has unacceptable ramifications.

## GUIDELINES

The following security issues should be considered when upgrading an OS:

a. An OS failure can have a cascading adverse effect on other systems and perhaps even the network.

b. System documentation and business continuity plans should be amended to reflect the OS upgrade.

c. Since OS upgrades typically affect many systems within an agency, such upgrades should be part of the annual maintenance plan/budget. OS upgrade testing and review cycles should also be included in this budget.

## Managing System Operations and System Administration

Systems shall be operated and administered using documented procedures that are efficient and effective in protecting the agency's data.

a. For IT transaction records, which include access and audit logs related to the activities of IT systems, agencies must establish and maintain an adequate system of controls.

b. For financial transactions and accounting records, the standard is addressed by the North Carolina Office of the State Controller.

c. Controls shall be employed and documented to provide for the management of system operations and system administration. To minimize the risk of corruption to operating systems or integrated applications, the controls shall include, but not necessarily be limited to, the following:

   i. Develop and document daily operational security procedures.

   ii. Assigned staff shall perform the updating of the operating systems and program/application backups.

   iii. Operating system software patches shall be applied only after reasonable testing verifies full functionality.

   iv. Physical or logical access shall be given to suppliers for support purposes only when necessary and with documented management approval. The suppliers' activities shall be continuously monitored.

   v. Vendor-supplied software used in operating systems shall be maintained at a level supported by the vendor.

d. Security responsibilities must be clearly defined for system administrators, who shall protect their assigned information technology resources and the information contained on those resources.

e. Appropriate training must be provided for system administrators.

f. System administrators shall do the following:

i. Ensure that user access rights and privileges are clearly defined, documented, and reviewed for appropriateness.

ii. Consider the risk of exposure when administering system resources.

iii. Take reasonable actions to ensure the authorized and acceptable use of data, networks and communications transiting the system or network.

## Scheduling System Operations

Modifications to information system operations shall be implemented and maintained properly.

a. Documented operational procedures must be created, implemented, and maintained during system operations and take into consideration the following:

   i. Computer start up, shutdown, and recovery procedures

   ii. Scheduling requirements (length, time frame, etc.)

   iii. Processes for handling errors and unforeseen issues that may arise during job execution

   iv. Contact lists

   v. System restrictions

   vi. Instructions for handling output, including failed jobs

   vii. Proper media handling and storage

   viii. Incident handling and escalation procedures

   ix. Configuration management

   x. Patch management

   xi. General system hardware and software maintenance

b. All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.

c. When special or emergency situations make it necessary to perform maintenance operations outside of the normal system operations schedule, these situations must be documented, management must be notified, and the operation processes used must be recorded.

d. Agencies shall develop change control procedures to accommodate resources or events that require changes to system operations.

e. Changes to system baselines require effective communication to ensure that information systems maintain secure operations and avoid lag due to processing consumption and to minimize downtime due to unforeseen problems during such changes.

f. Change control procedures must be documented and followed during the scheduled maintenance windows and take into consideration the following:
   i. Periods of maximum and minimum workflow.
   ii. The approval and notification process.
   iii. Interfaces with other applications, systems, or processes.
   iv. External agency and departmental interdependencies.
   v. Change categories, risk, and type.
   vi. The change request process.
   vii. Rollback plans and the point of no return.
   viii. Modifications to change control procedures for special or emergency circumstances.

g. All documentation shall be approved by management and reviewed on an annual basis for accuracy and relevancy.

h. Upon the completion of a baseline change, the audit change logs must be retained in accordance with the General Schedule for State Agency Records, Information Technology Records as established by the Government Records Section of the Department of Cultural and Natural Resources.

## Managing and Maintaining Backup Power Generators

Organizations with business requirements that demand uninterrupted information processing during power outages shall deploy backup power generators. When a backup generator is employed, the following requirements shall be observed:

a. Regularly inspect the generator to ensure it remains compliant with both safety and manufacturer maintenance requirements and has an adequate supply of fuel.

b. Ensure the generator has the capacity to sustain the power load required by supported equipment for a prolonged period of time.

c. Ensure the generator is tested according to the manufacturer's specifications.

d. Backup generators are usually combined with an uninterruptible power supply to protect critical information technology systems that demand high availability. Such a combination both supports an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss, and can also provide continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption.

e. Contingency plans should include procedures to be followed in the event the backup generator fails.

### Managing and Using Hardware Documentation

Additional documentation shall be developed and maintained that details hardware placement and configuration, provides flowcharts, etc. to effectively manage their information assets.

a. User documentation and technical specifications of information technology hardware shall be retained.

b. Documentation shall be secured from unauthorized use and made readily available to support system maintenance and system support staff. Each organization shall identify and record its information technology (IT) hardware assets in a formal hardware inventory/register.

c. A process shall be developed to ensure that IT hardware is identified with organization-unique physical asset tags and that the inventory/register is kept up to date.

d. The formal hardware inventory should include only information that is available for public inspection.

## 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.

## 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 handling of media are responsible for adhering to this policy and with any local maintenance 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 data storage media protection program throughout the agencies. |
| **Agency Security Liaison** | The Agency Security Liaison is responsible for ensuring that assigned storage media is managed in compliance with State requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate operational security posture for agency controlled storage media. |
| **Data Owner** | The State CIO is the Data Owner for all state data except data owned by Federal agencies, the General Assembly, the Judicial Department, and the University of North Carolina (UNC) and its constituent institutions.<br>Other public officials who have programmatic responsibility for the information in records / files must assess risk, classify data, and define the level of protection for the information for which they are responsible and may assign data stewards. |

| | |
|---|---|
| **Data Steward** | Data stewards are staff with assigned or designated responsibility who have direct operational-level responsibility for information management. Data stewards are responsible for data access and policy implementation issues, and for properly labeling data. |
| **Data Custodian** | Data custodians are responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, back-up and recovery processes, granting access privileges to system users as authorized by data stewards, or their designees, and implementing and administering controls over the information. |
| **Data User** | Data users are individuals who need and use data as part of their assigned duties or in fulfillment of assigned roles or functions. Individuals who are given access to medium- and high-risk data have a position of special trust and as such are responsible for protecting the security and integrity of the data. |
| **Information System Owner** | The Information System Owner (SO) is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |
| **Third Parties** | Third party service providers handling storage media containing sensitive data are responsible for managing storage media in a secure manner, in accordance with this policy. |

## MP-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 Media Protection controls at the organization, process and/or system level for all information assets / State data.

a. Information must be maintained in a manner that protects its security and integrity while making it available for authorized use.

b. Security measures must be implemented commensurate with the potential risk to individuals or institutions from unauthorized disclosure or loss of integrity.

c. Users of confidential information must observe and maintain the conditions imposed by the providing entity regarding confidentiality, integrity, and availability if legally possible.

Media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, mobile devices including portable storage media such as USB memory sticks and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, tablets, smartphones and cellular telephones digital cameras, and audio recording devices and non-digital media (e.g., paper, microfilm).

All data classifications must be reviewed at a minimum of every year or when there is a significant change that may impact the security posture of the data and/or system requiring a re-evaluation. A significant change includes but is not limited to data aggregation/commingling or decoupling of

data. A re-evaluation may also occur when a system classified as low or medium risk is later interconnected with a system classified as high risk.

The State has adopted the Media Protection security principles established in NIST SP 800-53, "Media Protection" control guidelines as the official policy for this security domain. The "MP" designator identified in each control represents the NIST-specified identifier for the Media Protection control family. The following subsections in this document outline the Media Protection requirements that each agency must implement and maintain in order to protect the privacy and security of sensitive information and to prevent the unauthorized use or misuse of agency data.

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.

## MP-2 – Media Access

Access to all digital and non-digital media shall be restricted to authorized individuals only, using State-defined security measures. Organizations may, at their discretion, restrict the use of removable media in their environments.

a. Security controls shall be put in place to protect the confidentiality and integrity of data contained on removable storage media from unauthorized disclosure and modification throughout the life of those storage media, including disposal.

Access controls shall include physical protection of and accountability for removable media to minimize the risk of damage to data stored on the removable storage media, theft, unauthorized access of data stored on the media, and software licensing violations

b. Assessment of risk must guide the selection of media, and associated information contained on that media requiring restricted access.

c. System Owners must document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

d. Processes shall be documented that ensure the protection of the information of media and restrict the information on the media from authorized access. This includes but is not limited to backup media such as tapes or disks or non-digital media.

e. Individuals must use only organizational approved devices to store Restricted or Highly Restricted data. Personally owned removal devices must not be used on the State Network and for storing non-public data:

i. All removable media must be encrypted using FIPS 140-2 approved encryption algorithms (e.g., AES 256), unless the Agency CIO or designee has classified the data as public. This includes, but is not limited to devices such as thumb/flash drives, external/removable hard drives, compact disks, magnetic tapes etc.

ii. All removable devices must be isolated and scanned for malware (malicious software) prior to use on the State Network. Autorun capabilities should be deactivated to reduce any risk of malware leak.

iii. Any detected malware must be removed from the media. The media must then be verified to ensure that it is safe for use on the State Network.

### Using Data Loss Prevention (DLP)

All preventive measures shall be used to ensure that the confidentiality, integrity of confidential data remains intact. Data Loss Prevention (DLP) technologies offer automated ways to protect confidential data from being transmitted external to the State Network without being approved and using encryption technologies. Automated tools must be employed to monitor internally or at network boundaries for unusual or suspicious transfers or events of the following data types:

i. Personally Identifiable Information (PII)

ii. Federal Tax Information (FTI)

iii. Protected Health Information (PHI)

iv. Payment Card Industry (PCI)

v. Criminal Justice Information (CJI)

vi. Family Educational Rights and Privacy Act (FERPA)

## MP-3 – Media Marking

a. All data must be labeled to reflect its classification. Recipients of information must maintain an assigned label and protect the information.

b. If a storage volume or information source contains multiple classifications, then the highest classification shall appear on the label. Data labeling may be automated where technically configurable, or it may be done manually.

c. If known, the applicable statute shall be cited on the label. For example, “Low Risk / Restricted per N.C.G.S. 132-6.1(c)”.

d. Agencies must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives, and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating “Federal Tax Information”.

e. The following table summarizes labeling requirements for different classes of data.

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

| MEDIA | Classification | | |
|---|---|---|---|
| | Low Risk | Medium Risk (Restricted) | High Risk (Highly Restricted) |
| **Electronic Media Email/text Recorded Media CD/DVD/USB (Soft Copy)** | No Label Required | Creation Date<br>Applicable Statute, if known i.e. "RESTRICTED per N.C.G.S. §132.6.1(c)<br>External **and** Internal labels<br>Email – Beginning of Subject Line<br>Physical Enclosure - Label | Creation Date<br>Applicable Statute, if known i.e. "HIGHLY RESTRICTED per N.C.G.S. §132.6.1(c) External **and** Internal labels<br>Email – Beginning of Subject Line<br>(See IRS 1075 for additional marking requirements for FTI) |
| **Hard Copy** | No Label Required | Each page if loose sheets; Front **and** Back Covers **and** Title Page if bound | Each page if loose sheets; Front **and** Back Covers **and** Title Page if bound |
| **Web Sites** | No Label Required | Internal Website Only<br>Each page labeled "RESTRICTED" on top **and** bottom of page | Internal Website Only<br>Each page labeled "HIGHLY RESTRICTED" on top **and** bottom of page |

## Data Classification

All data must be classified into one of three classes: 1) Low Risk, 2) Medium Risk, or 3) High Risk. Each is described below.

The classes determine the level of security that must be placed around the data. The data creator or steward, defined in **Responsibilities**, is responsible for classifying information correctly.

If data or systems include multiple classifications, the classification must default to the highest level. For example, a system that stores, processes, transfers, or communicates Low Risk and Medium Risk data is classified as Medium Risk.

**Low Risk** – Data that is open to public inspection according to state and federal law, or readily available through public sources.

By default, data is Low Risk unless it meets the requirements for a higher classification.

**Medium Risk (Restricted)** – Includes data that, if breached or disclosed to an unauthorized person, is a violation of state or federal law. Medium Risk data and systems may also be referred to as Restricted.

The following types of data must be classified as Medium Risk, at a minimum. This is not a complete list and is subject to legislative changes.

a. **State Employee Personnel Records** – Information that is confidential pursuant to N.C.G.S. 126-22. Any unauthorized discussion, disclosure, and/or dissemination of confidential applicant/employee information is a misdemeanor under N.C.G.S. 126-27

b. **Trade Secrets** – Trade secrets are defined in N.C.G.S. 66-152, and generally comprise information that is owned by a person, has independent value derived from its secrecy and which the owner takes measures to protect from disclosure. Misuse or misappropriation of a trade secret provides the owner a right of civil action (N.C.G.S. 66-153). The declaration of "trade secret" or "confidential" must be made at the time of the information's initial disclosure to a public agency (N.C.G.S. 132-1.2)

c. **Student Records** – The Federal Educational Rights and Privacy Act (FERPA) generally prohibits the improper disclosure of personally identifiable information derived from education records.

d. **Security Features** – Information that describes security features of electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes, is confidential under N.C.G.S 132-6.1(c)

e. **Sensitive Public Security Information** – As defined in N.C.G.S. 132-1.7, sensitive public security information includes information containing specific details of public security plans and arrangements or the detailed plans and drawings of public buildings and infrastructure facilities. Plans to prevent or respond to terrorist activity, to the extent such records set forth vulnerability and risk assessments, potential targets, specific tactics, or specific security or emergency procedures, the disclosure of which would jeopardize the safety of governmental personnel or the general public or the security of any governmental facility, building, structure, or information storage system, are also sensitive public security information.

By law, information relating to the general adoption of public security plans and arrangements, and budgetary information concerning the authorization or expenditure of public funds to implement public security plans and arrangements, or for the construction, renovation, or repair of public buildings and infrastructure facilities are not sensitive public security information and should be classified as Low Risk.

**High Risk (Highly Restricted)** – Data that, if breached or disclosed to unauthorized users, has the potential to cause great harm or damage to individuals or institutions. High Risk information can be disclosed only under very specific conditions, if at all. State or federal law or other requirements often include specific standards for protecting High Risk data and systems. High Risk data and systems may also be referred to as Highly Restricted. High Risk data includes the following:

a. **Personal Information and Personally Identifiable Information (PII)** – Under state law, personal information is a person's first name or first initial and last name **in combination with** other identifying information (N.C.G.S. 75-61(10)): Identifying information is defined by state law as the following:

   i. Social security or employer taxpayer identification numbers
   ii. Driver's license, state identification card, or passport numbers
   iii. Checking account numbers
   iv. Savings account numbers
   v. Credit card numbers
   vi. Debit card numbers
   vii. Personal Identification (PIN) Code as defined in N.C.G.S. 14-113.8(6)
   viii. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
   ix. Digital signatures
   x. Any other numbers or information that can be used to access a person's financial resources
   xi. Biometric data
   xii. Fingerprints
   xiii. Passwords
   xiv. Parent's legal surname prior to marriage (N.C.G.S. 14-130.20(b), N.C.G.S. 132-1.10)
   xv. Federal law also restricts the use of personal information by state motor vehicle agencies (18U.S.C. 2721 – Driver's Privacy Protection Act )

The following table summarizes the PII and Sensitive PII. **Note:** The table is not exhaustive.

| **PII includes:** Name, email address, home address, telephone number | |
|---|---|
| **Sensitive PII includes the following:** | |
| ***If stand-alone*** | ***If paired with the above identifiers*** |
| Social Security Number (SSN) | Citizenship or immigration status |
| Employer taxpayer identification numbers | Position description and performance plans without ratings |
| Driver's license or State ID # | Medical information |

| | |
|---|---|
| Passport Number | Ethnic or religious affiliation |
| Alien Registration Number | Sexual orientation |
| Financial account numbers (banking, credit, debit, etc.), or any other numbers or information that can be used to access a person's financial resources. | Account passwords |
| Biometric identifiers | Last 4 digits of SSN |
| Personal Identification (PIN) Code as defined in N.C.G.S. 14-113.8(6). | Date of birth |
| Digital signatures | Criminal history |
| Biometric data. | Mother's maiden name |
| Fingerprints | Electronic identification numbers |
| Passwords | Internet account numbers, or Internet identification names |

b. **State and Federal Tax Information** (FTI) – FTI is any return or return information received from the Internal Revenue Service (IRS) or secondary source, such as from the Social Security Administration (SSA), Federal Office of Child Support Enforcement, or the Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information. State and local tax information is defined in N.C.G.S. 132-1.1. Federal tax information is defined in IRC 6103 (b)(1).

c. **Payment Card Industry (PCI) Data Security Standard (DSS)** – PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates

d. **Personal Health Information (PHI)** – PHI is confidential health care information for natural persons related to past, present, or future conditions, including mental health information. This information is protected under the same controls as Health Insurance Portability and Accountability Act (HIPAA) of 1996 and state laws that address the storage of confidential state and federal personally identifiable health information that is protected from disclosure

e. **Criminal Justice Information (CJI)** – CJI applies to confidential information from Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including but not limited to biometric,

identity history, biographic, property, and case and incident history data. Criminal Justice Information is defined in the Criminal Justice Information Services (CJIS) Security Policy.

f. **Social Security Administration Provided Information** – Information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data as identified in paragraph (a) under **High Risk (Highly Restricted)**.

The following table summarizes the three data classes, Low Risk, Medium Risk (Restricted), and High Risk (Highly Restricted).

| | Data Classification | | |
|---|---|---|---|
| | **Low Risk** | **Medium Risk (Restricted)** | **High Risk (Highly Restricted)** |
| **Description** | Information not specifically made confidential by State or Federal law | Information made confidential by State or Federal law. This could include certain conditions such as when combined with other data. | Information made confidential by State or Federal Law that has the potential to cause great harm or damage to individuals or institutions if breached or disclosed to unauthorized users |
| **Types** | Information on publicly-accessible websites<br>Routine correspondence, email and other documents | Confidential personnel records<br>Trade Secrets<br>Security Features<br>Sensitive Public Security Information<br>FERPA | Personally Identifiable Information<br>PCI Data Security Standards<br>PHI/HIPAA<br>Criminal Justice Information<br>State and Federal Tax Information<br>Social Security Administration Provided Information<br>Attorney-client communications |

## System Classes

Systems are classified based on the data stored, processed, transferred, or communicated by the system and the overall risk of unauthorized disclosure. The following are the System Classifications:

**Low Risk System** – Systems that contain only data that is public by law or directly available to the public via such mechanisms as the Internet. Desktops, laptops and supporting systems used by agencies are Low Risk unless they store, process, transfer or communicate Medium Risk or High Risk data.

Low Risk systems must maintain a minimum level of protection as outlined in the State of North Carolina Statewide Information Security Manual, e.g., passwords and data at rest restrictions. Low risk systems are also subject to State laws and may require legal review to ensure that only public data is released in response to a public records request.

Breaches of Low Risk systems can potentially pose significant risk to the State. Websites with high visibility are often targets of opportunities for compromise and defacement. In addition, an unauthorized user may be able to pivot to a higher classified system. However, this policy is confined to data classification requirements.

**Medium Risk System** – Stores, processes, transfers or communicates Medium Risk data or has a direct dependency on a Medium Risk system. Any system that stores, processes, or transfers or communicates PII is classified as a Medium Risk system, at a minimum.

**High Risk System** – Stores, processes, transfers or communicates High Risk data or has a direct dependency on a High Risk system.

## MP-4 - Media Storage

Proper storage of data and information files shall be ensured.

a. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse.

b. All applicable statutory and regulatory requirements for data retention, destruction, and protection shall be met.

c. Organizations shall protect the State's information and comply with the organization's records retention policy or the General Schedule for State Agency Records, Information Technology Records.

d. Encryption keys shall be properly stored (separate from data) and available, if needed, for later decryption. When using encryption to protect data, the statewide information security standard for encryption shall be followed.

e. Change management procedures shall be established for the emergency amendment of data that occurs outside normal software functions and procedures.

f. All emergency amendments or changes shall be properly documented and approved and shall meet all applicable statutory and regulatory requirements.

g. Media containing FTI shall be physically controlled and securely stored.

h. Information system media shall be protected until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

i. Data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices, e.g., backups) shall be encrypted as required for the protection of the highest level of information contained therein.

j. Stored public data shall be kept to a minimum of what is necessary to adequately perform their business functions. Sensitive or confidential data that is not needed for normal business functions, such as the full contents of a credit card magnetic strip or a credit card PIN, should not be stored. Organizations should consider implementing a process (automatic or manual) to remove, at least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the agency's data retention policy.

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

### Media Archival

Agencies shall consult with the NC Department of Natural and Cultural Resources, Government Records Section, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived. In addition, the following requirements must be met:

a. When archiving data associated with legacy systems, agencies should plan to provide a method of accessing those data.

b. Classification of the back-up media so the sensitivity of the data can be determined.

c. Storage of media back-ups in a secure location, preferably an off-site facility.

d. All back-up media are physically secured from theft and destruction.

e. Migrating data to another system or archiving data shall be in accordance with applicable records management regulations and policies for potential future access.

## MP- 5 – Media Transport

All users must observe the requirements for transferring or communicating information based on its sensitivity, which are defined in the tables below. Data stewards, or their assigned representatives, may designate additional controls to further restrict access to, or to further protect, information:

a. Access to data shall be granted only after a business need has been demonstrated and approved by the data steward.

b. Transmittals or an equivalent documented tracking method must be used to ensure FTI and other Restricted or Highly Restricted data reaches its intended destination.

c. Media are transported by secured courier or other delivery method that can be accurately tracked.

d. Management approval shall be obtained before moving any media from a secure area.

e. Inventory logs of all media shall be properly maintained, and an inventory of all media logs, shall be performed at least annually.

The following table shows authorized methods for the transfer or communication of data.

| Method of Transfer or Communication | Classification | | |
|---|---|---|---|
| | **Low Risk** | **Medium Risk (Restricted)** | **High Risk (Highly Restricted)** |
| **Copying** | No Restrictions | Permission of Data Custodian Advised | Permission of Data Custodian Required |
| **Storage** | Encryption Optional | Encryption or physical access control**<br>No external agency cloud storage*** | Encryption required<br>No external agency cloud storage*** |
| **Fax** | No Restrictions | Encryption Required | Encryption Required |
| **Electronic Mail** | Encryption Optional | Encryption Required | Encryption Required |
| **Spoken Word*** | No Restrictions | Reasonable precautions to prevent inadvertent disclosure | Active measures to control and limit information disclosure to as few persons as possible |
| **Tracking Process by Log** | No Restrictions | Data Custodian is required to include audit trails for all access anddestruction of information. | Data Custodian is required to include audit trails for all access and destruction of information.<br>(See IRS 1075 for additional storage requirements for FTI) |
| **Granting Access Rights** | No Restrictions | Data Custodian or Designee Only | Data Custodian or Designee Only |
| **Post (Mail)** | No Restrictions | Physical Access Control | Physical Access Control<br>(See IRS 1075 for additional storage requirements for FTI) |

| | | | |
|---|---|---|---|
| **Release to a Third Party** | Third party must be an authorized user and have a job related need**** | Third party must be an authorized user and have a job related need**** | Third party must be an authorized user and have a job related need**** |

* Spoken word in the table is defined as transmission over mobile phone, voice mail, and answering machines as well as face-to-face.

** Any mobile computing device and portable computing devices such as personal digital assistants (PDAs), smart phones, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct the public's business, must use FIPS 140-2 validated encryption to protect all PII and confidential information that is stored on the device from unauthorized disclosure. It is highly recommended that physical locations with weak access controls, such as satellite offices, deploy full-disk encryption of Restricted and Highly Restricted data.

*** Pursuant to N.C.G.S. 143B-1335(b), no external cloud storage is allowed unless explicitly authorized by the State CIO.

**** Authorized users are users that have been granted access to the State of North Carolina Information Systems per the State of North Carolina Statewide Information Security Manual. Restricted information is restricted to authorized individuals who require access to the information as part of their job responsibilities per the State of North Carolina Statewide Information Security Manual. **Note**: Third party access to federal data may be restricted through federal mandates.

## MP-6 – Media Sanitization

Before disposal or re-use, media must be sanitized in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, *Guidelines for Media Sanitization.* These methods ensure data is not unintentionally disclosed to unauthorized users. Media containing Highly Restricted data shall be sanitized prior to disposal, release out of agency control, or release for reuse using agency approved sanitization techniques. The baseline for sanitizing media is shown in the table below.

| Sanitization | Classification | | |
|---|---|---|---|
| | **Low Risk** | **Medium Risk (Restricted)** | **High Risk (Highly Restricted)** |
| | Not Required (Recommended) | Mandatory | Mandatory |

When an agency authorizes a third party or cloud vendor to destroy State data, all data shall be permanently deleted and shall not be recoverable, in accordance with NIST Special Publication 800-88 revision 1, and certificates of destruction shall be provided to the agency.

### Media Disposal

Data confidentiality and integrity shall be protected through proper disposal of obsolete equipment and by using secure software disposal techniques.

All disposal of records must follow all federal and state laws including, but not limited to, the North Carolina General Schedule for State Agency Records, any agency program retention schedules and in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, Guidelines for Media Sanitization.

The following table summarizes disposal methods for the three data classifications. Though there are no specific restrictions for the disposal of Low Risk data, shredding is generally recommended as a best practice.

| Disposal | Classification | | |
|---|---|---|---|
| | **Low Risk** | **Medium Risk (Restricted)** | **High Risk** |
| | No restrictions (Optional) | Shredding, degaussing or secure disposal | Shredding, degaussing or secure disposal |

## MP-7 – Media Use

Security controls shall be in place to protect the confidentiality and integrity of the State's data stored on information system storage media throughout the life of those storage media, including disposal:

a. Access controls shall include physical protection of and accountability for removable media to minimize the risk of damage to data stored on the removable storage media, theft, unauthorized access of data stored on the media and software licensing violations.

b. Prohibit the connection of any non-State or agency owned information system data storage media, mobile device, or computers to a State-owned resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.

c. Prohibit the use of portable storage devices in agency systems when such devices have no identifiable owner.

d. The use of sanitization-resistance media that does not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices is prohibited for use with Highly Restricted data. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

e. Acceptable Use Policies (AUPs) shall define the proper use of information assets and shall include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage and Internet usage.

### Aggregation and Commingling

Commingling of differing classifications of data on the same media must be prohibited. All attempts must be made to ensure that there is a physical separation of the different data types within the same media. When deemed impossible, the data must be classified and labeled appropriately to the highest classification level with the most stringent security controls implemented.

When data with different classifications is gathered and summarized; and thus aggregated, the highest classification must be applied to all the aggregated data.

## MP-7 (1) – Media Use – Prohibit Use Without Owner

The use of portable storage devices in State information systems shall be prohibited when such devices have no identifiable owner. Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

## MP-8 – Media Downgrading (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.

## 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 physical and environmental security requirements.

| Role | Definition |
|---|---|
| **Senior Management** | Senior Management (the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designating organizational official) is responsible for the sponsorship, dissemination, development and support of the Physical security and environmental protection program., |
| **Security Liaison** | The Security Liaison is responsible for ensuring that physical and environmental risks are managed in compliance with the State's requirements by collaborating with organizational entities.<br>Liaisons are responsible for maintaining the appropriate operational security controls required for physical and environmental protection. |
| **Facility Management** | The Facility Manager, Facility Team, or other designated organizational official at management level, are responsible for site security and ensuring the facility is safe for occupancy. The Facility Manager may also have some responsibilities for authorization credentials, keys, physical access devices, etc. |

| | |
|---|---|
| **Third Parties** | Third party service providers are responsible for providing physical and environmental security in accordance with this policy. |

## PE-1 – Policy and Procedures

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data shall 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 Physical and Environmental Protection controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the Identification and Authentication security principles established in NIST SP 800-53, "Physical and Environmental Protection" control guidelines as the official policy for this security domain. The "PE" designator identified in each control represents the NIST-specified identifier for the Physical and Environmental Protection control family. The following subsections in this document outline the Physical and Environmental Protection requirements that each agency shall implement and maintain in order to protect the privacy and security of sensitive information and to prevent the unauthorized use or misuse of agency data.

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.

## PE-2 – Physical Access Authorizations

Access to digital and non-digital media shall be restricted to authorized individuals only, using State-defined security measures.

a. Access policies shall be developed for authorized individuals as well as visitors to State facilities.

b. Assessment of risk shall guide the selection of media, and associated information contained on that media requiring restricted access.

c. System Owners shall document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

d. Authorization credentials (e.g., badges, identification cards, and smart cards) shall be issued to everyone accessing a restricted area.

i. The level of access provided to each individual shall not exceed the level of access required to complete the individual's job responsibilities.

ii. The level of access shall be reviewed and approved before access is granted.

iii. Keys, badges, access cards, and combinations shall be issued to only those personnel who require access.

iv. Everyone within a State building must display either a State Identification (ID) Badge or a numbered and current visitor badge. These badges are the property of the State and are provided to employees and visitors as a convenience. Badges must always be visible above the waist when inside state government buildings. Badges must not be visible to the public outside of state government buildings (e.g., restaurants, retail stores, etc.).

v. Keys, combinations, and other physical access devices shall be secured at all times to prevent unauthorized access to agency facilities and assets. These shall also be inventoried on an agency-defined frequency. The unauthorized duplication of keys is prohibited. All requests for duplicate keys shall be submitted to the State locksmith for review, approval, and fulfillment.

vi. Keys shall be retrieved from the employee when they retire, terminate employment, or transfer to another position.

vii. Keys and combinations shall be changed at least annually for secure areas housing systems with Highly Restricted or FTI data.

viii. Authorizations and requirements for access shall be coordinated with facility and personnel security managers, as required or needed.

e. Access lists and authorization credentials shall be reviewed and approved quarterly to ensure the following:

i. Access shall be limited to only authorized personnel

ii. The level of access provided to each individual shall be consistent with the individual's job responsibilities

iii. Access rights shall be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides

f. Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where Restricted or Highly Restricted data is received, processed, stored, or transmitted.

## PE-3 – Physical Access Control

Sites and facilities that will be staffed and will house information technology equipment shall be carefully evaluated to identify and implement suitable controls to protect staff and agency resources from environmental threats, physical intrusion and other hazards and threats.

a. Organizations shall safeguard sites, buildings and locations housing its information technology assets.

b. All locations that house Restricted or Highly Restricted data shall be designed and secured in accordance the information being protected.

c. Physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit Restricted or Highly Restricted data reside shall be enforced by the following:

   i. Verifying individual access authorizations before granting access to the facility.

   ii. Controlling ingress/egress to the facility using physical access control systems/devices or guards.

d. Authorized individuals may include State and agency employees, contractors, vendors and customers.

e. Physical access controls should include some form of visible identification such as a Driver License or some other picture identification, e.g., agency badge. An audit trail of physical access for all individuals to data centers shall be maintained including entry and exit dates and times.

f. The number of people who have physical access to areas housing computer equipment shall be controlled to reduce the threats of theft, vandalism, and unauthorized system access. The following measures should be considered to control and restrict access to computing facilities:

   i. Access shall be restricted to people with authorized purposes for visiting the computer area.

   ii. Instructions shall be issued to visitors explaining security requirements and emergency procedures.

   iii. Visitors shall be escorted and should wear visible identification that clearly draws attention to their restricted status.

   iv. Where appropriate, organizations shall store resources in lockable storage cupboards where the physical security controls are sufficient to protect the equipment from theft.

   v. Lockable file cabinets shall be used to store Restricted or Highly Restricted data such as paper documents and computer media in a manner that is commensurate with the information's classification status.

g. Video cameras and/or access control mechanisms shall be used to monitor individual physical access to sensitive areas.

h. The use of personal cameras, video recorders and mobile computing devices shall be restricted from high security locations to protect the information being stored.

i. Duress alarms shall be used in areas where the safety of personnel is a concern. Alarms shall be provisioned to alert others such as staff, the police department, the fire department, etc.

j. Videoconference calls where Restricted or Highly Restricted information will be discussed shall be made in an area that is secured (e.g., offices or conference rooms where the door can be closed, and conversations cannot be overheard through thin walls).

k. Facilities that will house Restricted or Highly Restricted data shall include, but not limited to, the following security measures:

   i. Clearly defined, layered security perimeters to establish multiple barriers

   ii. Walls (of solid construction and extending from real ceiling to real floor where necessary)

   iii. Card-controlled gates and doors

   iv. Bars, alarms, locks, etc.

   v. Bollards

   vi. Video cameras and intrusion security system

   vii. Staffed reception desk

   viii. Fire doors on a security perimeter shall be equipped with alarms as well as devices that close the doors automatically.

## PE-4 - Access Control for Transmission

Physical access to information system distribution and transmission lines within agency facilities shall be controlled:

a. Protective measures to control physical access to information system distribution and transmission lines shall include the following:

   i. Locked wiring closets

   ii. Disconnected or locked spare network jacks

   iii. Protection of cabling by conduit or cable trays

b. Publicly accessible network jacks in data centers shall provide only Internet access by default unless additional functionality is explicitly authorized.

c. Physical access to networking equipment and cabling shall be restricted to authorized personnel.

## PE-5 - Access Control for Output Devices

Physical access to information system output devices, such as computer monitors, facsimile machines, copiers, and printers, shall be controlled to prevent unauthorized individuals from obtaining the output:

a. Where technically configurable, enable security functionality on printers, copiers and facsimile machines that requires users to authenticate with the device via a PIN or hardware token to access the device.

b. Control physical access to output devices by placing devices in controlled areas with keypad access controls or limiting access to individuals with certain types of badges.

c. Control physical access to monitors through the uses of privacy screens or by re-positioning monitors away from view by unauthorized users.

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

## PE-6 – Monitoring Physical Access

Physical access to information systems shall be monitored to detect and respond to physical security incidents:

a. Coordination with facility management and personnel security management personnel shall occur when responsibilities are in different organizations

b. Physical access logs shall be reviewed at least semi-annually by the agency Security Liaison or other designated agency official at management level.

c. Investigations of apparent security violations or suspicious physical access activities shall be conducted. Investigations and results of reviews shall be coordinated with the organization's incident response capability:

   i. Remedial actions identified as a result of investigations shall be developed and implemented.

   ii. Incident investigations shall follow the Incident Response Policy SCIO-SEC-308 for requirements on incident response.

d. Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities shall be part of the agency's incident response procedures.

e. Operational procedures shall be developed to document how these individuals shall respond to physical access incidents.

## PE-6 (1) – Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment

Physical intrusion alarms and surveillance equipment shall be installed and monitored. Automated mechanisms to recognize potential intrusions and initiate designated response actions shall be employed.

## PE-7 – Visitor Control

Withdrawn: Incorporated into PE-2 and PE-3.

## PE-8 – Visitor Access Records

Security access logs of areas housing information technology equipment shall be actively monitored:

a. Visitor access records for agency owned computing facilities shall address the following requirements:

   i. Name and organization of the person visiting
   ii. Signature of the visitor
   iii. Picture ID has been verified, and by whom, i.e. guard's initials
   iv. Date of access
   v. Time of entry and departure
   vi. Purpose of visit
   vii. Name of person visited
   viii. The visitor access records shall be reviewed at least semi-annually
   ix. Anomalies in visitor access should be reported to the organization's facility management.

b. Visitor access records for facilities housing FTI shall be maintained for five (5) years. All other facilities access records shall comply with the State's records retention policies.

## PE-9 – Power Equipment and Cabling

Power equipment and cabling for information systems shall be protected from damage and destruction:

a. Multiple electric feeds shall be employed to avoid a single point of failure in the power supply that are physically separated to help ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.

b. Both power and communication lines should be protected.

c. Automatic voltage controls for critical system components shall be employed to help ensure that power continues to flow in the event voltage fluctuates to unacceptable levels and causes damage to the information system component.

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

## PE-10 – Emergency Shutoff

The capability of shutting off power to the information system or individual system components in emergency situations shall be provided.

a. Emergency power switches shall be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency.

b. The locations for emergency power shutoffs must be documented.

c. All necessary personnel must be informed of the emergency power shutoff locations, and they must be trained to operate them safely.

d. Emergency procedures must be readily available to relevant personnel.

e. The emergency power-off capability must be protected from accidental or unauthorized activation.

f. Emergency shutoff switches are located in a visible location and clearly labeled.

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

## PE-11 – Emergency Power

Critical information technology systems shall be protected from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems continue to perform during power outages and electrical anomalies (e.g., brownouts and power spikes):

a. The three primary methods for providing continuous power are as follows:

   i. Multiple electric feeds to avoid a single point of failure in the power supply

   ii. Uninterruptible power supply (UPS)

   iii. Backup generator(s)

b. Each organization shall examine the availability requirements for critical equipment and determine which combination of these three methods best meets the needs of the organization.

c. Emergency power requirements for critical systems shall be analyzed based on the following best practices:

   i. Use of a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges. **Note**: Most UPS batteries do not last for more than four (4) hours without a continuous supply of power.

   ii. Contingency plans that include procedures to follow if the UPS fails.

   iii. Periodic inspections of UPS equipment to ensure that the equipment has the ability to sustain, for a predefined period, the power load of the systems and equipment it supports and is serviced according to the manufacturer's specifications.

d. Backup generators shall be used in combination with an UPS when requirements demand high availability and continuous processing in the event of a prolonged power failure. Such a combination both supports an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss, and can also provide continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption. Organizations that require a backup generator should ensure the following:

   i. Contingency plans shall include procedures to follow in the event the backup generator fails.

   ii. Ensure the generator has the capacity to sustain the power load required by supported equipment for a prolonged period of time.

   iii. Ensure the generator is tested at least quarterly according to the manufacturer's specifications.

   iv. The generator is serviced regularly in accordance with the manufacturer's specifications, and it has an adequate supply of fuel.

   v. An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period.

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

## PE-12- Emergency Lighting

Emergency lighting shall be provided in case of a main power failure:

a. Automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility shall be employed and maintained.

b. The automatic emergency lighting systems shall be tested annually to ensure they are fully operational.

c. The results of the test shall be documented.

## PE-13 – Fire Protection

Security controls shall be implemented to assure continual service of critical production systems, including controls that alert, monitor, and log intrusions, fires, explosives, smoke, water, dust, vibrations, chemicals, and electrical effects, electrical supply interferences, and electromagnetic radiation. This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and network closets:

a. Organizations shall install and maintain fire detection and suppression devices that are supported by an independent power source, such as a dry pipe sprinkler system.

b. Where appropriate, agencies shall provide fire-resistant storage for documents and media containing information critical to their business function.

c. Most file cabinets are not fire, smoke, or water safe and a fire-proof safe may not be water safe and may render any information that is stored in the cabinet or safe unusable; therefore, organizations shall consider storing duplicate copies of information at alternate locations.

d. Fire extinguishers must be checked annually, and the inspection date must be documented on the extinguisher.

e. All fire protection resources must be tested annually in accordance with local or state fire regulations to ensure they can be successfully activated in the event of a fire.

## PE-13 (1) – Fire Protection | Detection Systems - Automatic Activation and Notification

Fire detection devices/systems should activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire when the facility is not staffed on a continuous basis.

## PE-14 – Environmental Controls

a. Automatic temperature and humidity controls shall be implemented and maintained in data centers to prevent fluctuations potentially harmful to equipment.

b. Temperature and humidity monitoring shall be employed that provide an alarm or other notification of when temperature and humidity settings are exceeded due to heating, ventilation, or air conditioning (HVAC) failures and may adversely impact information assets.

## PE-15 –Water Damage Protection

a. Organizations shall include measures to prevent water damage in the design requirements for secure data storage.

b. The facility must have master shutoff valves that are accessible, working properly, and known to key personnel, to protect the information system from damage resulting from water leakage.

## PE-16 – Delivery and Removal

Access to delivery areas (e.g., loading docks and warehouses) shall be restricted and possibly isolated from the information system and media libraries to effectively enforce authorizations for entry and exit of information system components.

a. All types of information system components and packages that are delivered to or removed from the facility shall be authorized and controlled.

b. Records of those items entering and exiting the facility shall be maintained.

## PE-17 – Alternate Work Site

Organizations shall provide readily available alternate work locations (e.g., governmental offices, commercial locations, employee homes, etc.) as part of contingency operations:

a. Alternate work sites should be determined, approved, and documented.

b. The effectiveness of controls at alternate work sites shall be assessed, as feasible. Alternate work sites shall be equipped with any equipment needed to resume temporary operations such as telecommunications services such as alternative telephone services, wireless networking, satellite, radio that will allow employees to communicate with information security and privacy personnel in case of security incidents or problems.

c. Organizations shall secure and protect communications with information resources while personnel are working at off-site locations. Remote access security requirements are defined in the Access Control Policy, Section AC-17 – Remote Access.

d. Alternate work sites must meet state and federal security control requirements. If the organization does not have direct control over the remote location, the organization shall enter a contract with the owner of the remote location that stipulates the access controls and protection the owner shall implement. The following shall be implemented for alternate work sites:

    i. Sufficient physical access controls (e.g., doors, locks, etc.) to the site and to the agency's data store.

ii. Design requirements for secure data storage (e.g., fire suppression and detection equipment, heating, ventilation, and air conditioning [HVAC], measures to prevent water damage, etc.).

iii. Equipment being used or stored at an individual alternate work site, such as hotel, home, or other alternate site, must be secured when not in use.

iv. Equipment transported in vehicles must be hidden from casual view.

v. Equipment must not be stored in vehicles overnight.

vi. NIST SP 800-46, Revision 2 must be used as guidance for security in telework and remote access.

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

## PE-18 – Location of System Components

Information system components must be positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

This control is optional for LOW risk information systems.

## PE-19 – Information Leakage (Optional Control)

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

## PE-20 – Asset Monitoring and Tracking (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.

| | Security Planning Policy | Document No. SCIO-SEC-312 |
|---|---|---|

| Effective Date | Review Date | Version | Page No. |
|---|---|---|---|
| 01/29/2018 | 03/26/2025 | 4 | 1 of 5 |

## 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 Information Security Officer (SCISO) 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.

## 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. 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.

## 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.<br>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. |

## 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.
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.

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:

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.

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.

## Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. They 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.

This policy document provides the State of North Carolina's (State) risk assessment policy statements and commitment to develop, implement, maintain a Risk Assessment Policy, conduct annual risk and security assessments on all State information systems to help understand and identify all current threats, vulnerabilities and gaps within their process that may create critical risks availability, confidentiality and integrity for information systems and data of which the State is considered the owner.

## 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 that are included in IT risk assessment activities are responsible for adhering to this policy and with any local Risk Assessment requirements.

| Role | Definition |
|---|---|
| **Senior Management** | Senior Management (the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designating organizational official) is responsible for the sponsorship, dissemination and support of the Risk Management Plan and process, participating on the Risk Management Council, the review and approval of risk assessments and control recommendations and reporting to the SCRO what mitigation actions have been taken. |

| | |
|---|---|
| **State Chief Information Security Officer** | The State Information Security Officer (SCISO) as delegated by the State CIO is assigned the responsibility for the continued development, implementation, and maintenance of the risk management program. |
| **Risk Management** | The Enterprise Security and Risk Management Office (ESRMO) is responsible for governing the overall Security and Risk Management process, reviews presented Risk Assessment Reports and approves risk treatment plans or recommended controls. |
| **Security Liaison** | Security Liaisons are responsible for conducting the risk assessments, analyzing the risk and recommends controls, presenting risks for approval, documenting the process, and managing and facilitating the implementation of recommended controls. |
| **System Owner / Administrator** | System Owners/Administrators are responsible for participating in the identification and analysis process, participating on the Risk Management Council and for the implementation of technical controls. |
| **Functional Managers** | Managers in the functional areas are responsible for participating in the risk identification and analysis process, providing some participation on the Risk Management Council, and for the implementation of administrative controls. |

## RA-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 NIST SP 800-53, Security and Privacy Controls. Agencies shall manage risks appropriately. This document addresses the requirements set forth by the State to implement the family of Risk Assessment security controls at the organization, process and/or system level for all information assets / State data. Risk management includes the identification, analysis, and management of risks associated with an agency's business, information technology infrastructure, the information itself, and physical security to protect the state's information technology assets and vital business functions:

a. The State of North Carolina recognizes that each agency, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to the state's citizens.

b. The risk management program must identify and classify risks and implement risk mitigation as appropriate.

c. The program must include the identification, classification, prioritization, and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.

d. In general, "risk" is defined as a condition or action that may adversely affect the outcome of a planned activity. Some types of risk are as follows:

i. Business risk – The cost of and/or lost revenue associated with an interruption to normal business operations

ii. Organizational risk – The direct or indirect loss resulting from one or more of the following:

1. Inadequate or failed internal processes
2. People
3. Systems or external events

iii. IT risk – The loss of an automated system, network or other critical information technology resource that would adversely affect business processes.

iv. Legal risk – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.

v. Reputational risk – General estimation, by the public, on how state services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement).

vi. Citizen Services risk – Program services mandated by charter, legislation, or policy that provides for the delivery of state's business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.).

To meet the intent of N.C.G.S 143B-1376, ESRMO has developed a Continuous Monitoring Plan which requires that all agencies complete an annual risk and security assessment of their critical systems and infrastructure and that there are ongoing processes in place to assess the current posture of the environment. The Continuous Monitoring Plan is designed as a three-year program to ensure that all agencies are assessed using one or a combination of assessment methods identified below:

a. Third Party Independent Assessment
b. Self-Assessment

All agencies must complete a risk and security assessment annually. It is the agency's responsibility to ensure that an appropriate budget amount is requested to meet the ends of the legislative mandate. The Department of Information Technology (DIT), ESRMO may conduct compliance readiness reviews with the Executive Branch agencies to validate cyber readiness.

Within 30 days of completion of an assessment, all agencies are required to provide the ESRMO with the results and submit a plan to remediate the findings in the Enterprise Governance, Risk and Compliance (EGRC) tool. This tool will be used to create and maintain corrective actions plans for those deficiencies noted during a risk assessment, including vulnerability scans, and will ensure:

a. Accurate reporting on the status of corrective actions

b. Development of a process to evaluate supporting documentation and the time to monitor recommendations

Agencies shall coordinate with the ESRMO to address residual risks for those controls that cannot be implemented.

The State has adopted the Risk Assessment security principles established in NIST SP 800-53, "Risk Assessment" control guidelines as the official policy for this security domain. The "RA" designator identified in each control represents the NIST-specified identifier for the Risk Assessment control family. The following subsections in this document outline the Risk Assessment requirements that the State and each Agency must implement and maintain 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.

## Risk Management Program Activities:

The Risk Management program at a minimum shall focus on the following four types of activities:

a. **Identification of Risks**: A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.

b. **Analysis of Risks**: An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.

c. **Mitigation Planning**: Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For moderate or high rated risks, mitigation plans should be developed, documented, and assigned to managers. Plans should include assigned manager's signatures.

d. **Tracking and Controlling Risks**: Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

## Business Continuity Risk Management Processes:

For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt agency business. Agencies should identify the potential impacts in order to develop the strategies and justify the resources required to provide appropriate level of continuity

initiatives and programs. Agencies should conduct business risk impact analysis activities that include the following:

a. Define the agency's critical functions and services

b. Define the resources (technology, staff, and facilities) that support each critical function or service

c. Identify key relationships and interdependencies among the agency's critical resources, functions, and services

d. Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact

e. Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service

f. Estimate financial losses over time of each critical function or service

g. Estimate tangible (non-financial) impacts over time of each critical function or service

h. Estimate intangible impacts over time of each critical function or service

i. Document any critical events or services that are time-sensitive or predictable and require a higher- than-normal priority (For example - tax filing dates, reporting deadlines, etc.)

j. Identify any critical non-electronic media required to support the agency's critical functions or services

k. Identify any interim or workaround procedures that exist for the agency's critical functions or services.

l. Assess the professional capability of third parties and ensure that they provide adequate contact with the agencies and meet the agency's RTO and RPO requirements. Review dependence on third parties and take actions to mitigate risk.

m. Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.

## Security Risk Process:

The focus of security risk management is an assessment of those security risk outcomes that may jeopardize agency assets and vital business functions or services. Agencies should identify those impacts to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical agency functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize agency critical functions and services. Security risk impact analysis activities include the following:

a. Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for agency functions or services.

b. Identification of confidential information stored in the agency's files and the potential for fraud, misuse, or other illegal activity.

c. Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical agency functions and services.

d. Identification of the processes used to monitor and report to management on whatever applications, tools, and technologies the agency has implemented to adequately manage the risk as defined by the agency (e.g., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).

e. Identification of agency's IT Change Management and Vulnerability Assessment processes.

f. Identification of security mechanisms in place to preserve and protect the confidentiality, integrity and availability of State data and systems (e.g., encryption, PKI, etc.).

## RA-2 – Security Categorization

Organizations must address the following requirements:

a. Systems and the information processed, stored, transmitted, and received by them shall be categorized in accordance with applicable State and Federal laws, policies, regulations, standards, and guidance. NIST SP 800-60 Volumes 1 and 2 serves as a guidance for the categorization process. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the confidentiality, integrity, and availability of the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The impact to the Agency, State, personnel, and other external entities must be considered during the security categorization process.

b. System Owners need to be involved with the security categorization of an information system if they are responsible for the following:

   i. Any interconnected system dependencies, e.g., systems that share information
   ii. A system that may inherit a security control from their respective system

c. Include the security categorization process as a part of the system development lifecycle (SDLC). The security categorizations shall be developed early in the initiation stage ensuring the planning and implementation of the appropriate security controls throughout the SDLC

d. Verify the security categorization decision is reviewed and approved by the authorized or designated representative

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

f. The Business Owner, System Owner and supporting security liaison must assist with the development of the security categorization

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any agency of State government. The State's information shall be classified and handled in a manner that protects the information from unauthorized or accidental disclosure, modification, or loss. State Agencies must use the North Carolina Department of Information Technology Data Classification and Handling Policy for detailed requirements for the storage, labeling, classification and destruction of State data.

In addition, a Privacy Threshold Analysis (PTA) form shall be completed for each system, State or cloud hosted, that will contain State data. A PTA is the official State document that records the privacy sensitivity of a system that will host State data.

## RA-3 – Risk Assessment

Risk assessments consider risks posed to State agency operations and assets, or individuals from external parties, including but not limited to entities such as Service providers; Contractors operating information systems on behalf of the Agency; Individuals accessing State data and information systems; and Outsourcing organizations.

Organizations shall identify threats to and vulnerabilities in the system as part of the Risk assessment process.

Organizations must conduct security/risk assessments to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits and any related information.

Organizations must also conduct privacy/risk assessments to evaluate the level of risk, including the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

Organizations shall integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.

Organizations shall conduct security/risk assessments at minimum annually, or whenever there are significant changes to the critical information system or environment of operation or other conditions that may impact the security or privacy state of the system.

For State Agencies, an agency-wide third-party assessment of all critical systems (Restricted or Highly Restricted) and associated security controls will be conducted at a minimum every 3 years. Agencies that completed an agency-wide third-party assessment in year 1, may opt to complete a self-assessment or a more targeted and system specific assessment during years 2-3.

a. All assessment results will be provided to the ESRMO within thirty (30) days of completion. Risk assessment results shall be documented in Security and Privacy plans. The assessment shall include, at a minimum, the following:
    i. The rate of compliance with the enterprise-wide security standards.
    ii. An assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security.
    iii. Estimate the cost to implement the security measures needed for agencies to fully comply with the standards.
b. The risk assessment must consider risks posed to State's operations, assets, or individuals from external parties, including but not limited to the following:
    i. Organizations such as foreign nations and business competitors that may have an interest in information supplied to the agencies.
    ii. Service Providers:
        1. Contractors operating information systems on behalf of the State
        2. Individuals accessing the State's information systems
        3. Outsourcing entities/organizations (e.g., cloud service providers (CSPs))
            i. Agencies need to obtain prior approval from the State CIO before contracting with cloud-hosted solutions or off-site hosting.
            ii. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval.
            iii. Agencies shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Examples of acceptable attestation reports include Federal Risk and Authorization Management Program (FedRAMP) certification, Service Organization

Controls (SOC) 2 Type 2, ISO/IEC 27001 Information Security Management Standard, and HITRUST CSF (Common Security Framework).

iv. Procurement language must also require, in addition to initial validation, cloud/vendor must annually provide the agency validation of their continued compliance. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS). Examples of acceptable assessment reports include Federal Risk and Authorization Management Program (FedRAMP) certification, Service Organization Controls (SOC) 2 Type 2, ISO/IEC 27001 Information Security Management Standard, and HITRUST CSF (Common Security Framework). CSPs must demonstrate to the State that continuous monitoring activities are in place and compliance is being met. **Note**: SaaS vendors cannot use IaaS/PaaS certifications unless the application is explicitly covered as part of those assessments.

c. When planning and budgeting for security/risk assessments, the Agency must follow these requirements:

   i. Multi-year planning and budgeting techniques must be used.

   ii. Annual assessments must be included in information system budgets and planning.

   iii. Other significant, planned activities must be considered in budgets and planning (e.g., life cycle activities, enhancements, audits) to ensure cost effective use of resources.

   iv. All information systems in an agency must be considered to ensure resource efficiencies.

   v. Assessments must be coordinated between information systems with security control inheritance and other relational dependencies.

   vi. Agencies shall conduct an assessment using NIST 800-53 controls that includes at a minimum their critical systems.

   vii. An agency may perform an annual self-assessment of their organization or systems for two of the years out of a three year period. An independent third-party assessment shall be completed at least once every three (3) years.

   viii. An independent assessor or assessment team shall assess the security controls in the information system using an ESRMO provided assessment template.

d. A Plan of Action and Milestones (POA&M) or Corrective Action Plan (CAP) for the system documenting the planned, remedial actions to correct weaknesses or deficiencies in security and privacy controls and to reduce or eliminate known vulnerabilities must be developed.

e. The existing POA&M or CAP must be updated weekly for any critical/high risk findings of weaknesses and monthly for any medium/low risk findings of weaknesses including, but not limited to, the following:

   i. Reviews, tests, audits, or assessments

   ii. Security and Privacy impact analyses

   iii. Independent verification and validation findings

   iv. Continuous monitoring activities

   v. Incidents

f. All findings, recommendations, and their source must be tracked to the related item in the POA&M or CAP.

g. Findings must be analyzed as to their level of risk (e.g., high, medium, low) and a determination must be made for appropriate action(s) to be taken to correct or mitigate, as appropriate, the identified weaknesses to an acceptable level of risk.

h. One or more tasks to remediate a finding must be documented in the POA&M or CAP for any of the following:

   i. Critical-level risks that are not remediated within 7 days

   ii. High-level risks that are not corrected within 21 days

   iii. Medium-level risks that are not corrected within 30 days

   iv. Low level risks as required by the Agency CIO and that are not corrected within 90 days

i. All findings must be entered into a corrective action plan (CAP).

## Risk Assessment/Analysis

Risk assessment or analysis is the act of determining the probability that a risk will occur and the impact that event would have if it does occur. This analyzes the cause and effect of each possible event. Once risks have been identified and documented, risk analysis must be performed. During the risk analysis process, each potential risk event will be evaluated for the following:

a. The probability that the risk will occur
b. The impact of the risk if it occurs

These two factors of assessing the risk involving probability and impact shall be measured for probability using a scale of Low, Medium, and High, and giving each an associated number.

For impact, the State shall use a qualitative method for analysis as it is typically a quicker and usually more cost-effective way to analysis risks. Analysis will be performed with the goal of gathering data on the following:

a. The likelihood of the risk occurring
b. The qualitative impact on the company, system, or data
c. The quality of the risk data being utilized

Business Risk Analysis of each business system shall be utilized to assist in impact determination.

## Impact Definitions

| Magnitude of Impact | Impact Definition |
|---|---|
| High | If an event could be expected to have a severe or catastrophic adverse effect on agency operations, agency assets, or individuals; and cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets. |
| Medium | If an event could be expected to have a serious adverse effect on agency operations, agency assets or individuals, and cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs. |
| Low | If an event could be expected to have a limited adverse effect on agency operations (including mission, functions, image or reputation, agency assets, or individuals; and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs. |

As Risks are identified and quantified, they are entered into the into the DIT Enterprise Governance Risk Compliance (EGRC) reporting and tracking tool. All risks are reported based on type of risk, probability, impact, and overall risk. To determine and quantify the overall risk, the below table (based on NIST 800-30) is used.

| **Threat Likelihood** | **Low** (10) | **Medium** (50) | **High** (100) |
|---|---|---|---|
| **High** (1.0) | **Low** 10 x 1.0 = 10 | **Medium** 50 x 1.0 = 50 | **High** 100 x 1.0 = 100 |
| **Medium** (0.5) | **Low** 10 x 0.5 = 5 | **Medium** 50 x 0.5 = 25 | **Medium** 100 x 0.5 = 50 |
| **Low** (0.1) | **Low** 10 x 0.1 = 1 | **Low** 50 x 0.1 = 5 | **Low** 10 x 0.1 = 10 |

## Risk Response

For each identified risk, a response must be identified. The Agency Security Liaison will select a risk response for each risk. The probability and impact of the risk will be the basis of recommending which actions should be taken to mitigate the risk. During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed.

**Avoid:** Risk avoidance involves changing aspects of the overall business process or system architecture to eliminate the threat.

**Transfer:** Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat it simply makes another party responsible for managing it. This would include identifying avenues of insurance, etc.

**Mitigate:** Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.

**Accept:** Risk acceptance should normally only be taken for low-priority risks. All risks should have a recommendation of control(s) and / or alternative solutions to mitigate risk.

| Risk Level | Risk Description and Necessary Actions |
|---|---|
| **High** | Mandatory need for corrective measures. CAP must be in place for 60 days. |
| **Medium** | Plan must be developed to mitigate corrective measures within 90 – 120 days. |
| **Low** | Decision on whether to implement corrective measures or accept the risk. |

## Use of Independent Assessors

When assessments must be conducted by an entity with an explicitly determined degree of independence to the organization, independence must be determined by the Agency CIO based on the security categorization of the information system and/or the risk to Agency operations and assets, and to individuals.

To make an informed, risk-based decision, the selection of independent assessors must consider the following criteria to ensure credibility of the security assessment results and to receive the most objective information possible. Preserving the impartial and unbiased nature of the assessment process including, but not limited to, freedom from any perceived or actual conflicts of interest with respect to the following:

a. The development, operation, and/or management of the information system

b. The chain of command associated with the information system

c. The determination of security control effectiveness

d. A competitive relationship with any organization associated with the information system being assessed or impacts on their reputations

e. Undue influence as a result of a contractual or other related relationship

f. The assessor's technical expertise and knowledge of State and federal requirements

## RA-4 – Risk Assessment Update

Withdrawn: Incorporated into RA-3.

## RA-5 – Vulnerability Monitoring and Scanning

All State Risk Assessment programs must include the following requirements:

a. All malware (malicious software) scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events.

b. Monitoring and scanning for vulnerabilities in information systems and hosted applications must be performed at least every 7 days and when new critical vulnerabilities potentially affecting the system/applications are identified and reported if existing data does not allow for quick determination of affected systems. Vulnerability scanning shall include scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.

c. Real-time scanning for spyware, adware, and bots (software robots) with one or more anti-spyware programs that detect these malicious programs and help protect the system against infection.

d. Scan for malware on files that are downloaded from the Internet or any other outside source, including all external media, such as flash drives, CDs, etc. shall be conducted.

e. Viruses, spyware, Trojan applications, and other malicious code may cause damage to the State's infrastructure via Web browsers and therefore all internet traffic shall be scanned to prevent malicious code from infecting the State's infrastructure.

f. External computers or networks making remote connection to internal agency computers or networks shall utilize an agency-approved active virus scanning and repair program and an agency-approved personal firewall system (hardware or software). The agency shall ensure that updates to virus scanning software and firewall systems are available to users. Non-State computers or networks making a remote connection to a public Web server are exempted.

g. Organizations shall scan their networks and take remediation actions to identify any multifunctional devices (MFD)s on the network that are vulnerable and/or configured insecurely.

h. Conduct scanning independently or as a coordinated effort with ESRMO.

i. Prior to commencing vulnerability scanning efforts, the following should be addressed:

   i. Scanner selection – Evaluate the mandated tools for use within the respective environments

   ii. The network and host-based vulnerability scanner shall provide the following capabilities:

      1. Identify active hosts on networks.
      2. Identify active and vulnerable services (ports) on hosts.
      3. Identify vulnerabilities associated with discovered operating systems and applications

The ESRMO shall implement a suite of automated monitoring tools to effectively monitor and identify vulnerabilities on networked computer servers and workstations. Agencies shall utilize the tools provided by the ESRMO, if the agency tools are determined to duplicate functionality. Vulnerability monitoring tools and techniques are employed that promote interoperability among tools and automate parts of the vulnerability management process by using standards for the following:

i. Enumerating platforms, software flaws, and improper configurations

ii. Formatting and making transparent, checklists and test procedures

iii. Measuring vulnerability impact

iv. Analyzing vulnerability scan reports and results from vulnerability monitoring

v. Remediating legitimate vulnerabilities in accordance with the agency's assessment of risk and the established mitigation timeframes. Refer to Vulnerability Mitigation section below. See also Vulnerability Risk Ratings and Remediation section in System and Information Integrity Policy, SI-2 – Flaw Remediation.

vi. Employing vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned

Sharing information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).

## Vulnerability Management

System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application services and ports are enabled and opened in the system's firewall, as applicable. Vulnerabilities that threaten the security of the State's network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings:

a. Personnel shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches and updates, and eliminating or disabling unnecessary services.

b. Where possible tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) shall be used to test for the presence of vulnerabilities.

c. Perform scans, typically, on systems and networks known to be stable and preferably during times of least impact to the critical functionality of the system. Expect vulnerability scanning to occur during various phases of the system's life cycle.

## Vulnerability Mitigation

a. Vulnerability mitigation procedures must specify, at a minimum, the proposed resolution to address identified vulnerabilities, required tasks necessary to affect changes, and the assignment of the required tasks to appropriate personnel.

b. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available. When a vulnerability risk is 'high-level' and no patch is available, steps must be taken to mitigate the risk through other compensating control methods (e.g., group policy objects, firewalls, router access control lists). A patch needs to be applied when it becomes available. When a 'high-level' risk vulnerability cannot be totally mitigated within the requisite time frame, agencies need to notify agency management and the State Chief Information Officer of the condition.

c. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.

d. Appropriate notification shall be provided after vulnerability mitigation plans have been executed.

e. In the event of a zero-day vulnerability, a situation where an exploit is used before the developer of the software knows about the vulnerability, agencies shall mitigate the vulnerability immediately, if possible, and apply patches as soon as possible after the vendor provides them.

f. For vulnerability risk ratings and mitigation timelines, please refer to SI-2 – Flaw Remediation.

## Vulnerability Information Review and Analysis

a. Relevant vulnerability information from appropriate vendors, third party research, and public domain resources shall be reviewed on a regular basis.

b. Relevant vulnerability information, as discovered, shall be distributed to the appropriate personnel, including the security office.

c. Appropriate personnel shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

## Requirements for Compliance

a. Procedures must be developed to ensure the timely and consistent use of security patches and use a consistent vulnerability naming scheme to mitigate the impact of vulnerabilities in systems.

b. An explicit and documented patching and vulnerability policy is required, as well as a systematic, accountable, and documented set of processes and procedures for handling patches.

c. The patching and vulnerability policy shall specify techniques an organization will use to monitor for new patches and vulnerabilities and personnel who will be responsible for such monitoring.

d. An organization's patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches.

e. The process for handling patches shall include the following:

   i. Using organizational inventories

   ii. Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring (See http://cve.mitre.org)

   iii. Patch prioritization techniques

   iv. Organizational patch databases.

   v. Patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications

f. A list of sources of information about security problems and software updates for the system and application software shall be developed.

g. A procedure for monitoring those information sources shall be established.

h. Updates for applicability to the systems shall be evaluated.

i. The installation of applicable updates shall be planned.

j. Updates shall be installed using a documented plan.

k. New computers shall be deployed with up-to-date software.

l. After making any changes in a system's configuration or its information content, new cryptographic checksums or other integrity-checking baseline information for the system shall be created.

Agencies shall utilize the vulnerability management tools provided by ESRMO, if the agency tools are determined to duplicate functionality. The vulnerabilities to be scanned need to be readily updated as

new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

## RA-5 (2) – Vulnerability Monitoring and Scanning – Frequency of Updates

The list of system vulnerabilities scanned shall be updated prior to a new scan or when new vulnerabilities are identified and reported.

## RA-5 (5) – Vulnerability Monitoring and Scanning – Privileged Access

Privileged access authorization to an information system shall be implemented for vulnerability scanning activities. In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain Highly Restricted information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

This control is optional for LOW 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.

APPENDIX A – AGENCY ANNUAL ASSESSMENT AND COMPLIANCE REPORT TEMPLATE

[AGENCY LETTER HEAD]

TO: xxxx
State Chief Information Officer

FROM: [AGENCY]

SUBJECT: yyyy Agency Compliance Report

---

Pursuant to the authorities and powers of the State Chief Information Officer enumerated in Session Law 2015-241, and as Agency head for [AGENCY];

A. I certify that [AGENCY] has implemented the appropriate processes and procedures listed below to be in compliance with the Statewide Information Security Manual and State statues:

☐ No data of a confidential nature, as defined in the General Statutes or federal law, was entered into or processed through any information technology system or network established under this Article until safeguards for the data's security satisfactory to the State CIO have been designed and installed and are fully operational.

☐ Agency obtained approval from the State CIO prior to contracting for the storage, maintenance, or use of State data by a private vendor.

☐ Agency ensured all information technology security goods, software, or services purchased using State funds, or for use by a State agency or in a State facility, was subject to approval by the State CIO in accordance with security standards

☐ Agency completed annual risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies.

| Type of Assessment | Completion Date | Cost for Assessment |
|---|---|---|

| | | |
|---|---|---|
| [Enter 3rd party/vendor details or Self-Assessment] | | |

☐ Agency ensured all contracts for third party assessment and testing, was approved by the State CIO (as applicable) and resulting sanitized assessment reports were made public.

☐ Agency provided the full details of the State agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation

☐ Agency designated an agency liaison in the information technology area to coordinate with the State CIO.

☐ Agency completed an annual assessment of the agency's contracted vendors, to comply with the current security enterprise-wide set of standards. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security.

| Cloud Service Provider | Cloud Offering | Service Type | Review/Assessment Date |
|---|---|---|---|
| Ex. Microsoft | Office 365 | IaaS / SaaS / PaaS | |
| [Add Rows Needed] | | | |

☐ Agency submitted disaster recovery plans to the State CIO on an annual basis and as otherwise requested by the State CIO

| Business Continuity Plan (Review/Submission Date) | Business Continuity Test Date |
|---|---|
| | |

☐ Agency achieved completion rate ≥ 95 percent for annual Cybersecurity Awareness Training during CY 20XX

| Number of Employees (including contractors), involved | Number of Users who Completed the training | Training Budget Required |
|---|---|---|
| | | |

☐ [AGENCY] has not completed all requirements but have identified a plan to be in compliance. Attached is our assessment report to include corrective action plan indicating when the agency will meet these requirements.

B. In accordance with § 143B-1342, below is the estimated cost to implement security measures needed for agencies to fully comply with the standards.

SECURITY / BUDGET DEFICIENCIES:

| Security Gaps | Estimated Cost to Remediate | Agency budget approved? (Y/N) |
|---|---|---|
| Ex. Security boundary devices, Personnel, Training, Vulnerability Management, End of Life Support | | |

For additional information about this submission please contact: [INSERT AGENCY CONTACT]

_____ _____

Printed Name of Secretary/CIO or Designee [Date]

_____

Signature of Secretary/CIO or Designee

## 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 acquisition, development or operation of information systems and supporting infrastructure are responsible for adhering to this policy and with any local system and service acquisition 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 a secure information system and service acquisition program throughout the agencies. |
| **Agency Security Liaison** | The Agency Security liaison(s) are responsible for ensuring that information system and service acquisition requirements are managed in compliance with the State's requirements by collaborating with organizational entities.<br>Liaison(s) are responsible for maintaining the appropriate information system and service acquisition requirements required for information security protection. |
| **Information System Owner** | The Information System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |
| **Third Parties** | Third party service providers are responsible for implementing secure information systems, system components, and services. |

## SA-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 provides requirements for the system and service acquisition process which is required to assure that information systems are acquired using controls sufficient to safeguard the State's information systems. This document addresses the requirements set forth by the State to implement the family of System and Service Acquisition security controls at the organization, process and/or system level for all information assets / State data. Failure to protect network infrastructures against threats can result in the loss of data integrity, loss of availability of data, and/or unauthorized use of data or information systems of which State agencies are considered the owner.

The State has adopted the System and Service Acquisition principles established in National Institute of Standards and Technology (NIST) SP 800-53 "System and Service Acquisition" control guidelines as the official policy for this security domain. The "SA" designator identified in each control represents the NIST-specified identifier for the System and Service Acquisition control family. The following subsections in this document outline the system and service acquisition requirements that each agency must implement and maintain adhere to 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.

## SA-2 – Allocation of Resources

Organizations shall expediently allocate resources for information security to provide rapid yet supervised allocation, ensuring that the organization is modernized and protected against emerging and ongoing threats. Funding shall include allocation of resources for the initial system or system service acquisition, and funding for the sustainment of the system/service. The following items shall be done:

a. Determine the high-level security and privacy requirements for the system or service in each mission or business-process planning.

b. Identify, document, and allocate the appropriate amount of resources which are required to protect the system or service as part of the capital planning and investment control process.

c. Establish discrete line items for information security and privacy in the budgeting process.

## SA-3 – System Development Life Cycle

Organizations shall acquire, develop, and manage systems using a System Development Life Cycle (SDLC) that incorporates information security and privacy considerations:

a. Identify qualified individuals having information security and privacy roles and responsibilities that are involved in creating the SDLC. This may include the CIO, CISO, business owners, system administrators, security architects, security engineers, security analysts, etc. These personnel will ensure that the system life cycle activities meet the security and privacy requirements for the organization.

b. Define and document information security and privacy roles and responsibilities throughout the SDLC.

c. Integrate the agency information security and privacy risk management process into SDLC activities.

d. A business case justification of custom system development projects shall be required. When proposing the development of custom software, a strong business case shall include the following:

   i. Support the rationale for not enhancing current systems;

   ii. Demonstrate the inadequacies of packaged solutions; and

   iii. Justify the creation of custom software.

e. The organization shall implement a change management program which enables system engineers, architects, and security analysts to expediently perform their necessary business functions, yet maintain a controlled, secure, and functioning environment. Examples of this program include multi-tiered deployments (Dev, Test, Quality Assurance (QA), Production), which are capable of backing-up and rolling-back changes which are unsuccessful. Change control requirements are provided in the Configuration Management Policy, SCIO-SEC-305, Section CM-3.

f. The organization will plan for End-of-Life (EoL) and End-of-Support dates (EoS) for systems and services. This will ensure that systems and services can receive security patches and updates throughout the system development lifecycle, and that the organization is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured. See also CM-2 Baseline Configuration for more information about supported versions of products.

### GUIDELINES

a. Many SDLC models exist that can be used by an organization in developing an information system. A traditional SDLC is a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle. A general SDLC should include the following phases:

i. Initiation

ii. Acquisition / Development

iii. Implementation / Assessment

iv. Operations / Maintenance

v. Sunset (disposition)

b. Each of these five phases should include a minimum set of tasks to incorporate security in the system development process. Including security early in the SDLC will usually result in less expensive and more effective security than retrofitting security into an operational system.

c. The following questions should be addressed in determining the security controls that will be required for a system:

i. How critical is the system in meeting the organization's mission?

ii. What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?

iii. What regulations, statutes, and policies are applicable in determining what is to be protected?

iv. What are the threats that are applicable in the environment where the system will be operational?

v. What kinds of data will be used by the system?

## SA-4 – Acquisition Process

Security functional requirements are a part of the hardware, software, or firmware acquisition process. Agencies shall be capable of acquiring necessary solutions in an expedient manner in accordance with N.C.G.S. 143B-1350., The following shall be done.

a. Security and privacy functional requirements shall include security capabilities, security functions, and security mechanisms.

b. Strength of mechanism requirements based on security categorization, e.g., Low or Moderate, associated with such capabilities, functions, and mechanisms shall include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass.

c. Security and privacy assurance requirements shall include the following:

i. Development processes, procedures, practices, and methodologies;

ii. Evidence from development and assessment activities providing grounds for confidence that the required security and/or privacy functionality has been implemented and the required security strength has been achieved.

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements.

f. Requirements for protecting security and privacy documentation.

g. Description of the information system development environment and environment in which the system is intended to operate.

h. Acceptance criteria requirements for assessing the ability of a system component, software or system to perform its intended function.

i. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.

j. Proposed vendor hardware design shall comply with information security and other State policies and standard security and technical specifications, such as the following:

   i. Vendors shall configure the system with adequate capacity to fulfill the functional requirements stated in the agency's design document.

   ii. Vendor shall configure hardware security controls to adequately protect data. (Optionally, the vendor may assist the agency with the configuration of software security controls to provide adequate data protection on the vendor's hardware.)

k. Systems under consideration for acquisition shall be interoperable with the peripherals and systems currently in use.

l. To mitigate risks of exploitation of covert channels third-party applications shall be obtained from reputable sources.

m. Non-security functional and technical requirements shall be a part of the hardware, software, or firmware acquisition process.

n. Agencies shall follow State procurement policies when acquiring hardware to ensure that the purchase meets specified functional needs. Agencies shall include specific requirements for performance, reliability, cost, capacity, security, support, and compatibility in Requests for Proposals (RFPs) to properly evaluate quotes.

o. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval. This document is intended to help agencies reach a decision for a specific system that will meet the State's security and compliance requirements. A VRAR is required for both solutions hosted on State infrastructure and those that are not hosted on State infrastructure.

p. New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the agency.

## SA-4 (1) – Acquisition Process | Functional Properties of Controls

Developer(s) of the system, system component, or information system service shall provide a description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality (e.g., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

## SA-4 (2) – Acquisition Process | Design and Implementation Information for Controls

Developer(s) of a system, system component, or information system service shall provide design and implementation information for the security controls to be employed that includes the following: security-relevant external system interfaces, high-level design, source code, or hardware schematics.

## SA-4 (9) – Acquisition Process | Functions, Ports, Protocols, and Services in Use

Developer(s) of a system, system component, or information system service shall identify the functions, ports, protocols, and services intended for use.

## SA-4 (10) – Acquisition Process | Use of Approved PIV Products

Information technology products on the FIPS 201-approved products list shall be employed for Personal Identity Verification (PIV) capability implemented within agency systems.

## SA-5 – System Documentation

Organizations must obtain, develop, or document administrator and user documentation for the system, system component, or system service. Such documentation shall be distributed to designated agency officials that describes the following:

a. Secure configuration, installation, and operation of the system, component, or service.

b. Effective use and maintenance of security and privacy functions/mechanisms.

c. Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.

d. User-accessible security and privacy functions/mechanisms and how to effectively use those functions/mechanisms.

e. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.

f. What responsibilities the end user has in maintaining the security and privacy of the individuals.

The following shall also be done:

g. Ensure each new or updated system includes supporting system documentation and technical specifications of information technology hardware, whether the system is developed or updated by in-house staff or by a third-party vendor.

h. Create, manage, and secure system documentation libraries or data stores that are always available to only authorized personnel.

i. Ensure that system documentation is readily available to support the staff responsible for operating, securing, and maintaining new and updated systems.

j. Control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting and staff turnover.

k. All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.

## SA- 6 – Software Usage Restrictions

Withdrawn: Incorporated into CM-10 and SI-7.

## SA-7 – User Installed Software

Withdrawn: Incorporated into CM-11 and SI-7.

## SA-8 – Security and Privacy Engineering Principles

Organizations shall apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. Security and Privacy engineering principles shall be primarily applied to new development information systems or systems undergoing major upgrades. For legacy systems, organizations shall apply security engineering principles to system upgrades and modifications to the extent that it is technically configurable, given the current state of hardware, software, and firmware within those systems.

a. Security and Privacy engineering principles shall include the following:

   i. Developing layered protections;

   ii. Establishing sound security and privacy policy, architecture, and controls as the foundation for design;

   iii. Incorporating security and privacy requirements into the SDLC;

iv. Delineating physical and logical security boundaries;

v. Ensuring that system developers are trained on how to build secure software;

vi. Tailoring security and privacy controls to meet organizational and operational needs;

vii. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;

viii. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

b. NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems shall be used as guidance on engineering principles for information system security. NIST SP 800-160 may be found at the following link:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

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

## SA-9 – External System Services

Agencies shall require that third parties and providers of external system services comply with statewide information security and privacy requirements. Agencies shall employ controls as follows:

a. Define and document how external information system comply with statewide information security and privacy controls to include user roles and responsibilities and compliance auditing and reporting requirements. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval.

b. Monitor security and privacy control compliance by external service providers on an ongoing basis.

c. Restrict the location of information systems that receive, process, store, or transmit state and federal data to areas within the following areas:

i. US States,

ii. US Territories,

iii. US Embassies,

iv. US Military installations (stateside or overseas)

d. Agencies that outsource their information processing must ensure that the service provider demonstrates compliance with state standards and procedures, and industry quality standards.

e. Outsourcing agreements shall include the following:

i. The agency's course of action and remedy if the vendor's security and privacy controls are inadequate such that the confidentiality, integrity or availability of the agency's data cannot be assured.

ii. The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters.

iii. The vendor's ability to provide processing in the event of failure(s).

f. To support service delivery, the outsourcing agreements shall contain, or incorporate by reference, all the relevant security and privacy requirements necessary to ensure compliance with the statewide information security standards, the agency's record retention schedules, its security policies, and its business continuity requirements.

g. Services, outputs, and products provided by third parties shall be reviewed and checked, at minimum annually, in accordance with state statutes.

i. To monitor third party deliverables, agencies shall do the following:

a) Monitor third party service performance to ensure service levels meet contract requirements.

b) Review reports provided by third parties and arrange regular meetings as required by contract(s).

c) Resolve and manage any identified problem areas.

j. Contracts with vendors providing offsite hosting or cloud services that will host Restricted or Highly Restricted data must require the vendor to provide the State an independent, third-party risk assessment report (e.g., Service Organization Control (SOC) 2 Type II, International Organization for Standardization (ISO) 27001:2022, Federal Risk and Authorization Management Program (FedRAMP) Moderate), or HITRUST CSF (Common Security Framework)) before contract award and annually thereafter to establish compliance with state policy.

k. Any changes to services provided by a third party must be approved by the agency prior to implementation.

l. Agencies shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data.

m. Agencies shall ensure that the service-level agreement (SLA) includes requirements for regular monitoring, review, and auditing of the service levels and security requirements as well as incident response and reporting requirements. The SLA shall state how the service provider is responsible for data stored or shared with the provider.

n. Agencies shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. Agencies shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level.

o. Changes to an SLA and services provided shall be controlled through formal change management.

p. Agencies must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit Highly Restricted data, including federal tax information (FTI), unless explicitly approved by the Office of Safeguards.

## SA-9 (2) – External System Services | Identification of Functions/Ports/Protocols/Services

Providers of external system services shall identify the functions, ports, protocols, and other services required for the use of such services. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.

## SA-10 – Developer Configuration Management

System developers shall create and implement a configuration management plan that does the following:

a. Performs configuration management during system design, development; implementation, operation and/or disposal for the following:

   i. Internal system development and system integration of commercial software;

   ii. External system development and system integration;

b. Documents, manages, and controls changes to the system or configuration items; and the potential security and privacy impacts

c. Implements only agency approved changes to the system,

d. Documents approved changes to the system,

e. Tracks security flaws and flaw resolution within the system,

f. Organizations shall mitigate risks of exploitation of covert channels by protecting the source code in custom developed applications.

## SA-11 – Developer Testing and Evaluation

System developers shall test for software faults that pose a security risk at all post-design stages of the system development life cycle prior to putting an application into production. The following shall be done:

a. Develop and implement a security and privacy assessment plan;

   i. Develop and implement a plan that supports ongoing security and privacy assessments. Testing requirements must be defined and documented for both system development and system integration activities. The plan must include requirements for retesting after significant changes occur.

   ii. Perform security testing/evaluation.

      1. Restricted or Highly Restricted data shall not be used for testing purposes.

      2. Organizations may permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and policies. Data anonymization or data masking tools shall be used if available.

      3. If production data is used for testing, the same level of security controls required for a production system shall be used.

   iii. Produce evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation

   iv. Implement a verifiable flaw remediation process

   v. Correct flaws identified during security testing/evaluation

b. Teach and encourage software fault-reporting procedures through security training and awareness programs.

c. Designate a quality control team that consistently checks for faults and that is responsible for reporting them to software support.

d. Use a formal recording system for the following:

   i. Tracks faults from initial reporting through to resolution.

   ii. Monitors the status of reported faults and confirms that satisfactory resolutions have been achieved.

   iii. Provides reports and metrics for system development and software support management.

   iv. Software faults shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability

e. While faults are being tracked through to resolution, research shall also be conducted to ensure no security controls have been compromised and resolution activities have been appropriately authorized.

f. Perform unit, integration, and system regression testing/evaluation:

i. Require that information system developers/integrators perform a vulnerability assessment to document vulnerabilities, exploitation potential, and risk mitigations.

ii. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.

iii. To maintain the integrity of information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment.

iv. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment.

v. Qualified personnel must certify that the upgrade or change has passed acceptance testing.

vi. A rollback plan must be established in the event the upgrade or change has unacceptable ramifications.

g. The following issues and controls shall be included when developing acceptance criteria and acceptance test plans:

i. Capacity requirements - both for performance and for the computer hardware needed.

ii. Error response - recovery and restart procedures and contingency plans.

iii. Routine operating procedures - prepared and tested according to defined policies.

iv. Security controls - agreed to and put in place.

v. Manual procedures - effective and available where technically configurable and appropriate.

vi. Business continuity - meets the requirements defined in the business continuity plan.

vii. Impact on production environment - able to demonstrate that installation of new system will not adversely affect current production systems (particularly at peak processing times).

viii. Training - of operators, administrators, and users of the new or updated system.

ix. Logs - logs of results shall be kept for a defined period once testing is completed.

h. Implement a verifiable flaw remediation process to correct security weaknesses and deficiencies identified during the security testing and evaluation process.

i. Controls that have been determined to be either absent or not operating as intended during security testing/evaluation must be remediated.

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

## SA-12 – Supply Chain Protection (Optional)

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

## SA-13 – Trustworthiness (Optional)

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

## SA-14 – Criticality Analysis (Optional)

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

## SA-15 – Development Process, Standards, and Tools (Optional)

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

## SA-15 (3) – Development Process, Standards, and Tools – Criticality Analysis (Optional)

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

## SA-16 – Developer Provided Training (Optional)

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

## SA-17 – Developer Security Architecture and Design (Optional)

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

## SA-18 – Tamper Resistance and Detection (Optional)

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

## SA-19 – Component Authenticity (Optional)

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

## SA-20 – Customized Development of Critical Components (Optional)

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

## SA-21 – Developer Screening (Optional)

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

## SA-22 – Unsupported System Components

Agencies must replace system components, e.g., servers, workstations, laptops, applications, etc., when support for the components is no longer available from the developer, vendor, or manufacturer. Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

## 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.

| | System and Communications Protection Policy | Document No. SCIO-SEC-316 |
|---|---|---|

| Effective Date | Review Date | Version | Page No. |
|---|---|---|---|
| 01/29/2018 | 03/26/2025 | 4 | 1 of 21 |

## 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 implementation or operation of system and communications protection controls are responsible for adhering to this policy and with any additional local system and communications protection 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 a secure information system and communications protection program throughout the agencies. |
| **Agency Security Liaison** | The Agency Security Liaison is responsible for ensuring that information system and service acquisition requirements are managed in compliance with the State's requirements by collaborating with organizational entities.<br>Liaisons are responsible for maintaining the appropriate information system and communications protection required for information security protection. |
| **Information System Owner** | The Information System Owner (SO) is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |

| | |
|---|---|
| **Third Parties** | Third party service providers are responsible for ensuring that systems, system components and services they provide are secure and do not negatively impact security of pre-existing systems by implementing secure information system and communications protection practices in accordance with this policy. |

## SC-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 System and Communications Protection security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the System and Communications Protection security principles established in NIST SP 800-53, "System and Communications Protection" control guidelines as the official policy for this security domain. The "SC" designator identified in each control represents the NIST-specified identifier for the System and Communications Protection control family. The following subsections in this document outline the System and Communications Protection requirements that each agency shall implement and maintain in order to protect the confidentiality, integrity and availability of information and information systems by assuring systems, system components and services acquired are secure and do not negatively impact security of pre-existing systems used for conducting the agencies' mission critical business functions.

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.

## SC-2 – Separation of System and User Functionality

User functionality (including user interface services) shall be separated from information system management functionality in application components.

a. For the Application and Database secure zones, an approved firewall or other network segmentation mechanism, for example micro segmentation or virtual local area networks (VLANs), is required to segregate application servers and database servers.

b. Information systems shall prevent the presentation of information system management-related functionality at an interface for non-privileged users.

c. Internal network infrastructures (e.g., local area networks [LANs]) shall be segregated into network zones to protect application servers from the user LAN.

d. Production and non-production environments (e.g., test, development, QA, etc.) shall be segregated from one another.

e. Wireless networks shall be physically or logically segregated from internal networks such that an unknown external user cannot access an agency's internal network.

f. Systems not able to adhere to the DMZ and/or other security requirements of this policy need to be in a Special Assembly zone. Agencies must document the rationale for developing a Special Assembly zone.

i. An example of special assembly zones includes facility management systems, such as heating, ventilation, or air conditioning (HVAC), badge access, electrical generators, power distribution, water, and closed-circuit television (CCTV). These may be excluded from the network zoning requirements, provided those systems are not publicly accessible, are logically isolated (e.g., VLANs) from other networked systems and cannot access other shared systems/services, and have appropriate access control mechanisms in place.

g. Where technically configurable, virtual machines with Highly Restricted data shall be separated from those with unrestricted data.

## SC-3 – Security Function Isolation (Optional)

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

## SC-4 - Information in Shared System Resources

Information systems shall prevent unauthorized and unintended information transfer via shared system resources.

a. Information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) shall not be made available for object reuse or shall residual information be made available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

b. Information systems shall prevent unauthorized information transfer via shared resources in accordance with statewide information security standards when system processing explicitly switches between different information classification levels or security categories.

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

## SC-5 – Denial of Service Protection

The effects of denial of service (DoS) attacks shall be limited by appropriately securing all hosts that could be a potential target for a common DoS or a distributed denial of service (DDoS) attack. The following controls shall be implemented:

a. Denying all inbound traffic by default, thus limiting the channels of network attacks;

b. Periodically scanning network and devices for bots (software robots) and Trojan horse programs;

c. Deploying authentication mechanisms wherever technically configurable;

d. Designing and implementing networks for maximum resiliency;

e. Developing specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan;

f. Managing excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks;

g. Providing detection and monitoring capabilities to detect indicators of denial of service attacks against the agency and to determine if sufficient resources exist to prevent effective denial of service attacks.

h. Additional guidance is available NIST SP 800-61 Computer Security Incident Handling Guide.

## SC- 6 – Resource Availability (Optional)

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

## SC-7 – Boundary Protection

The following shall be done for boundary protection:

a. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with statewide security architecture and privacy requirements. Managed interfaces include, for example, gateways, routers, firewalls, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

b. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.

c. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency network.

d. Limit the number of external network connections to the information system. Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic.

e. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks ("subnets").

f. Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional demilitarized zone (DMZ—filtered subnet) environments.

g. Firewalls shall be configured to the following specifications:

   i. Local user accounts shall be configured on network firewalls, for the sole purpose of eliminating possible extended outages.

   ii. Local accounts shall be configured to only be used when the device cannot make contact with the central unit. During normal operation, the local account exists, but is not used.

   iii. Passwords on firewalls shall be kept in a secure encrypted form as required by the Identification and Authentication Policy SCIO-SEC-307, Section IA-5 Authenticator Management.

   iv. Agencies shall designate a minimum of two (2) authorized firewall administrators. At least one of the designated firewall administrators will be a security specialist who is consulted before firewall rule set changes are approved and implemented.

   v. For temporary or emergency port openings, the process shall establish a maximum time for the port to be open, which shall not exceed 5 days. The authorized firewall rule set administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.

   vi. System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.

   vii. Firewalls shall be installed in locations that are physically secure from tampering. Firewalls shall not be relocated without the prior approval of agency management.

   viii. Firewall rule sets shall always block the following types of network traffic:

      a) Unauthorized scanning activity that originates outside of its network, within its network, and between information systems.

      b) Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.

      c) Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.

      d) Traffic inbound to the State Network containing ICMP (Internet Control Message Protocol) traffic will be blocked at the perimeter with the following exceptions: To allow testing

initiated from internal IT support groups, ICMP echo replies and ICMP TTL expired will be permitted inbound to the State Network but will be limited to specific IP addresses or small subnets representing the internal support group. A ping point can be established at the perimeter, for troubleshooting purposes, with the sole purpose and sole capability of responding to a ping.

e) Inbound network traffic containing IP Source Routing information.

f) Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 and/or containing directed broadcast addresses.

ix. Logging features on State Network firewalls shall capture all packets dropped or denied by the firewall, and agency staff or the entity managing the firewall shall review those logs at least monthly.

x. Firewall rule implementation shall have an approval process that includes review by the Security Liaison, or designated personnel, of the agency that requires or no longer requires the rule. Existing firewall rules shall be reviewed every 6 months by the Security Liaison, or designated personnel, that is responsible for the application/device that requires the rule sets in question. For example, agency X application requires certain firewall rules to be implemented; therefore, that agency security liaison is responsible for approving and reviewing the firewall rules required for the application. Confirmation of the firewall rule review that is conducted every 6 months shall be sent to the ESRMO.

xi. Additional requirements for protecting Federal Tax Information (FTI) on networks are provided in IRS 1075 Section 3.3.6 Network Boundary and Infrastructure.

xii. Firewall configurations and associated documentation must be treated as restricted information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).

h. NIST SP 800-41 must be used as guidance on firewalls and firewall rule set.

i. NIST SP 800-189 must be used as guidance on routers.

j. NIST SP 800-77 must be used as guidance on Virtual Private Networks (VPNs).

k. NIST SP 800-94 must be used as guidance on IDPS.

## SC-7 (4) – Boundary Protection | External Telecommunications Services

The following shall be done:

a. Implement a managed interface for each external telecommunication service.

b. Establish a traffic flow policy for each managed interface.

c. Protect the confidentiality and integrity of the information being transmitted across each interface.

d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.

e. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit mission/business need.

f. Prevent unauthorized exchange of control plane traffic with external network.

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.

## SC-7 (5) – Boundary Protection | Deny by Default – Allow By exception

Protective controls shall at a minimum include the following:

a. Positive source and destination address checking to restrict rogue networks from manipulating the State's routing tables.

b. Firewalls must use an authentication mechanism that provides accountability for the individual and to ensure device configuration does not become corrupted with false entries.

c. Screen internal network addresses from external view.

d. Information systems at managed interfaces shall deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception, also known as whitelisting). This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

## SC- 7 (7) – Boundary Protection | Split Tunneling for Remote Devices

Information systems, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections (e.g., split tunneling) with the system and communicating via some other connection to resources in external networks.

## SC-7 (8) – Boundary Protection | Route Traffic to Authenticated Proxy Servers

Where technically configurable, routing agency-defined internal communications traffic to agency-defined external networks shall be achieved through authenticated proxy servers at managed interfaces, such as web content filtering devices.

## SC-8 – Transmission Confidentiality and Integrity

The confidentiality and integrity of transmitted information shall be protected during the transfer process.

a. Organizations shall implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling. The organization must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized personnel.

b. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic.

c. Controls shall be deployed to ensure resources do not contribute to outside-party attacks. These controls include the following:

   i. Securing interfaces between agency-controlled and non-agency-controlled or public networks.

   ii. Standardizing authentication mechanisms in place for both users and equipment.

   iii. Controlling users' access to information resources.

   iv. Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date.

d. Employees, contractors, and others performing work for the State shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access.

e. Employees, contractors, and others performing work for the State shall not use any utility, application, or service on a device used to access State systems that obfuscates or anonymizes user or device identity (e.g., IP address, MAC address, user identity, geographic location, etc.), except for authorized State-managed solutions. Prohibited services include, but are not limited to, the following: personal VPN, anonymizing/privacy features of a device or software, Private Relay, and Tor.

f. Each agency shall document and retain on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its unencrypted transmission to a party not served by the agency's internal network.

g. Organizations shall address the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the Internet, or exchange of electronic media and tapes.

h. Secure protocols, such as Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec) shall be used for secure network management functions.

i. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol version(s) utilizing TLS as per NIST SP 800-52 Rev 2. Any TLS version that is disallowed, or not otherwise covered with a 'shall' and

'should' or has reached the end of a deprecation period as per NIST SP 800-52 Rev. 2 shall not be utilized.

j. NIST SP 800-52 Rev. 2 must be used as guidance on protecting transmission integrity using TLS.

k. NIST SP 800-77 must be used as guidance on protecting transmission integrity using IPsec.

l. NIST SP 800-81 must be used as guidance on Domain Name System (DNS) message authentication and integrity verification.

m. NIST SP 800-113 must be used as guidance on SSL VPNs.

n. Instant messaging technologies, where allowed, must not be used to transmit any type of Restricted or Highly Restricted data.

o. The following types of transmission require enhanced protection (e.g., cryptography mechanisms) when integrity is an important consideration:

   i. Internal traffic within the information system and applications

   ii. Internal traffic between two or more information systems

   iii. External traffic to or across the Internet

   iv. Remote access

   v. Email

   vi. FTP transmissions

   vii. Web services

   viii. Voice over Internet Protocol (VoIP)

   ix. Audio and video

   x. Wireless client to host communications

p. Agencies shall protect the confidentiality of data transmitted on the network from corruption or data loss by prohibiting the extending, modifying, or retransmitting network services, such as through the installation of new switches or other network devices, unless prior Agency CIO or delegate approval is granted.

## SC-8 (1) – Transmission Confidentiality and Integrity | Cryptographic Protection

Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure of information and/or to detect changes to information during transmission.

## SC-9 – Transmission Confidentiality

Withdrawn: Incorporated into SC-8

## SC-10 – Network Disconnect

a. All sessions shall be terminated that have had no activity for a period of thirty (30) minutes or less, such that the user must re-authenticate his/her identity to resume the session.

b. An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the State Network.

c. The information system must be configured to disconnect inactive remote VPN.

## SC-11 – Trusted Path (Optional)

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

## SC-12 – Cryptographic Key Establishment and Management

Electronic key systems shall be managed according to the following requirements:

a. FIPS 140-2, or 140-3 where available, approved algorithms that do not have any known weaknesses shall be used when protecting Restricted or Highly Restricted data. Enablement of full FIPS mode in an application or operating system is not required. Organizations may optionally enable additional cipher algorithms for transport encryption if they are not considered legacy or disallowed by FIPS and do not have any known weakness. Known weaknesses are things such as, but not limited to, less than 128-bit for ciphers, weak configuration parameters that affect the whole, or a vulnerability. The following is provided as a quick reference list for common FIPS approved algorithms at the time of this writing:

   i. Block cipher algorithms: AES-128, AES-192, AES-256
   ii. Digital Signatures: RSA ≥ 2048, ECDSA or EdDSA ≥ 224
   iii. Hash functions: SHA-2 family (e.g., SHA-256), SHA-3 family (e.g. SHA3-256), TupleHash/ParallelHash only as per SP 800-185.

   Products and modules that have been validated by NIST as FIPS 140-2 compliant and are currently listed as validated products list may be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

b. Key-based data encryption systems must implement a key escrow system to guarantee access to encrypted data when needed. Key escrow data shall be routinely backed up. Recovery procedures must be tested at least annually to ensure access and availability to encrypted data.

c. Only authorized personnel shall have access to keys used to access Restricted or Highly Restricted data. Encryption keys must be properly stored (separate from data) and available, if needed, for later decryption. The following must also be ensured:

   i. Separation of duties or dual control procedures are enforced.

   ii. Any theft or loss of electronic keys results in the notification of management.

   iii. All keys are protected against modification, substitution, and destruction, and secret/private keys are protected against unauthorized disclosure.

   iv. Cryptographic keys are replaced or retired when keys have reached the end of their life or the integrity of the key has been weakened or compromised.

   v. Physical protection is employed to protect equipment used to synchronize, store and archive keys.

   vi. An electronic key management and recovery system, including all relevant key escrow procedures, is documented and in place. This shall be handled through key escrow procedures.

   vii. Custodians of cryptographic keys formally acknowledge they understand and accept their key-custodian responsibilities.

   viii. Encrypted data are recoverable, at any point in time, even when the person(s) who encrypted the data is no longer available.

d. NIST SP 800-56A and NIST SP 800-56B must be referenced as procedures, on establishing cryptographic keys.

e. NIST SP 800-57 must be referenced as guidance on managing cryptographic keys.

## SC-13 – Cryptographic Protection

Cryptographic modules must be implemented for cryptographic uses as described below. Cryptographic requirements for each specified cryptographic use shall be defined:

a. All laptops that are used to conduct State business shall use encryption to protect all information stored on the laptop's storage device.

b. All other mobile computing devices and portable computing devices such as smart phones, tablets, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct State business, shall use encryption to protect all Restricted and Highly Restricted data from unauthorized disclosure.

| Device | Encryption Requirements |
|---|---|
| Laptops, Notebooks, etc. | All devices shall use Full Disk Encryption (FDE) using a FIPS 140-2 Level 1 certified AES-256 encryption algorithm. |
| Mobile and portable computing devices, such as tablets, smart phones, and personal digital assistants. Removable Media such as CDs, DVDs, memory sticks (flash drives), tape media, or any other | All Restricted or Highly Restricted data shall be encrypted using a FIPS 140-2 Level 1 certified algorithm of at least 128-bit strength.<br><br>**Note**: Restricted and Highly Restricted State data should only be stored on State issued and State-owned media. |

c. Policies concerning the storage of the State's Restricted and Highly Restricted data on all portable and removable media devices shall be enforced.

d. For a list of validated cryptographic modules and products, refer to the following NIST publication: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

## SC-14 – Public Access Protections

Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10.

## SC-15 – Collaborative Computing Devices and Applications

The following shall be done when using collaborative computing devices and applications:

a. Prohibit remote activation of collaborative computing devices and applications, for example, networked white boards, cameras, and microphones.

b. Provide an explicit indication of use to users physically present at the devices. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

## SC-16 – Transmission of Security and Privacy Attributes (Optional)

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

## SC-17 – Public Key Infrastructure Certificates

a. Public key infrastructure certificates shall be issued or obtained from an approved service provider.

b. Registration to receive a public key certificate must include authorization by a supervisor or a responsible official.

c. Public key certificates must be issued by using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

d. Organizations shall include only approved trust anchors in trust stores or certificate stores managed by the organization.

e. Only digital certificates for transport encryption either issued by and/or approved by the State Certification Authority (managed by NCDIT) can be used on end-user facing State applications and/or systems as well as for system-to-system where external connections are accepted. For internal system-to-system transport encryption, internally signed certificates may be utilized so long as at minimum they adhere to algorithm requirements in SC-12(a), are valid for no longer than four years, and can be tracked and managed to prevent expiration.

f. NIST SP 800-32 must be used as guidance on public key technology.

g. NIST SP 800-63, Version 1.0.2 must be used as guidance on remote electronic authentication.

## SC-18 – Mobile Code

A tamper protection program shall be implemented for the information system, system component, or information system service to protect the State Network from mobile code that performs unauthorized and malicious actions. Refer to the Statewide Glossary of IT Terms for a definition of mobile code. The following are categories of mobile code/active content:

a. Category 1/high risk mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, server and remote system services and resources. These pose a significant risk to the State's information systems because they allow unlimited access to a user's computer. There are two subgroups of Category 1 mobile code technologies:

   i. Category 1 technologies can differentiate between signed and unsigned mobile code. The technologies can also be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. Category 1 mobile code technologies may be used by agencies when additional restrictions are implemented. The following are assigned to Category 1:

      - ActiveX controls
      - Shockwave movies (e.g., dcr, .dxr, .dir files), including Xtras, that execute in the Shockwave for Director plug-in.

   ii. Category 1 consists of mobile code technologies that are prohibited from use on State information systems beyond the local information system's authorization boundary, or to or from external entities because they cannot differentiate between signed and unsigned mobile code, nor can they be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code. The following are assigned to Category 1:

- Mobile code scripts that execute in Windows Scripting Host (WSH) (e.g., JavaScript or VBScript downloaded via URL file reference or email attachments)
- Hypertext Mark-up Language (HTML) applications (e.g., .hta files) that download as mobile code
- Scrap objects (e.g., .shs and .shb files)
- Microsoft Disk Operating System (MS-DOS) batch scripts
- UNIX shell scripts
- Binary executables (e.g., .exe files) that download as mobile code

ii. Category 1 mobile code must be obtained from a trusted source and must be signed with a State approved PKI code-signing certificate.

iii. All information systems capable of executing mobile code must be configured to disable the execution of unsigned Category 1 mobile code obtained from outside the organization-managed boundary.

b. Category 2/medium risk mobile code technologies have full functionality, allowing mediated or controlled access to workstations, server, and remote system services and resources. Category 2 technologies can pose a moderate security threat to the State's information systems because they offer limited control by the user on what the code is allowed to do. They may be used when the Category 2 restrictions described in Section 6, Procedures are implemented.

i. The following are assigned to Category 2:

- Java applets and other Java mobile code
- Visual Basic for Applications (VBA) (e.g., Microsoft Office macros)
- LotusScript (e.g., Lotus Notes scripts)
- PerfectScript (e.g., Corel Office macros)
- Postscript
- Mobile code executing in .NET Common Language Runtime

ii. Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel (i.e., TLS VPN, IPsec, or other approved by the ESRMO).

iii. Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, or network connections other than to its originating host).

iv. Where technically configurable, web browsers and other mobile code-enabled products must be configured to prompt the user prior to the execution of Category 2 code.

v. Where technically configurable, protections against malicious Category 2 technologies must be employed at end user systems and at system boundaries.

c. Category 3/low risk mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 mobile code may be freely used without restrictions in information systems. Category 3 technologies pose limited risk to the State's information systems because they are very restricted in the actions they can perform. The following are assigned to Category 3:

- JavaScript, including Jscript and European Computer Manufacturers Association (ECMA) Script variants, when executing in the browser
- VBScript, when executing in the browser
- Portable Document Format (PDF)
- Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash plug-in

d. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and therefore have not been assigned to one of the three risk categories described above. Emerging mobile code technologies must not be used unless approved by management. The download and execution of mobile code using emerging technologies must be blocked by all means available at the network boundary, workstation, host, and within applications.

## SC-19 – Voice Over Internet Protocol

a. Usage restrictions and implementation guidance shall be established for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

b. The use of VoIP within the information system shall be authorized, monitored, and controlled.

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

## SC-20 – Secure Name/Address Resolution Service (Authoritative Source)

Information systems shall require the following for domain name system (DNS):

a. Enable external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service using DNS servers.

b. DNS servers shall not be configured to allow zone transfers to unknown secondary servers.

   i. If an agency maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers

   ii. If an agency maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only

   iii. When a domain has a US extension (e.g., state.nc.us), the US Domain Registry requires the domain allow copies to be transferred to the US Domain Registry's Master Server. Therefore, all domains registered with US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry. When DIT maintains the DNS, agencies may request DIT to allow additional IP addresses to receive zone transfers. Agencies must work with DIT to define acceptable IP addresses and/or IP address ranges.

## SC-21 – Secure Name / Address Resolution Service (Recursive or Caching Resolver)

a. Information systems shall request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources using recursive resolving or caching domain name system (DNS) servers.

b. Recursion on an authoritative name server is prohibited.

## SC-22 – Architecture and Provisioning for Name / Address Resolution Service

Information systems that collectively provide name/address resolution service shall be fault-tolerant and implement internal/external role separation.

a. At least two authoritative domain name system (DNS) servers shall be deployed to eliminate single points of failure and to enhance redundancy. One configured as the primary server and the other configured as the secondary server.

b. Servers shall be deployed in two geographically separated network subnetworks (e.g., not located in the same physical facility).

c. Split DNS shall be used to prevent leaking internal system and IP information to external non-State clients to limit information exposure.

d. DNS servers with internal roles shall only process name and address resolution requests from within the organizations (e.g., from internal clients).

e. DNS servers with external roles only process name and address resolution information requests from clients external to organizations (e.g., on external networks including the Internet).

f. Clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists) shall be specified.

g. Servers must be configured to provide redundancy, load balancing and distributed access.

h. NIST SP 800-81 must be used as guidance on secure domain name system deployment.

## SC-23 – Session Authenticity

a. Information systems must protect the authenticity of communications sessions. Protection mechanisms shall be selected and implemented to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission. Mechanisms include but are not limited to the following:

- Security services based on IPsec
- VPNs
- TLS
- DNS
- SSH
- Digital signatures
- Digital certificates
- Digital time stamping
- FIPS 140-2 approved encryption technology

b. Information systems shall invalidate session identifiers upon user logout or other session termination to curtail the ability of adversaries from capturing and continuing to employ previously valid session IDs.

c. NIST SP 800-52 Rev. 2 must be used as guidance on the use of TLS mechanisms.

d. NIST SP 800-77 must be used as guidance on the deployment of IPsec VPNs and other methods of protecting communications sessions.

e. NIST SP 800-95 must be used as guidance on securing web services.

f. NIST SP 800-113 must be used as guidance on SSL VPNs.

## SC-24 – Fail in Known State (Optional)

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

## SC-25 – Thin Nodes (Optional)

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

## SC-26 – Decoys (Optional)

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

## SC-27 – Platform-Independent Applications (Optional)

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

## SC-28 – Protection of Information at Rest

Information systems shall protect the confidentiality and integrity of all Restricted or Highly Restricted data at rest. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

This control is optional for LOW risk information systems.

## SC-28 (1) – Protection of Information at Rest – Cryptographic Protection

a. Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure and modification of all Restricted or Highly Restricted data at rest: Restricted and Highly Restricted data stored in non-volatile storage (e.g., disk drive) on all endpoints shall be encrypted with FIPS 140-2 compliant encryption during storage (regardless of location).

b. Organizations shall consider increasing integrity protection of data by recording data onto hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R).

c. Organizations shall consider storing data at rest on a physically separate non-mobile storage device (e.g., disk drive, tape drive) with cryptographic protections in place.

d. Whereas a virtual machine may store or process confidential data, the virtual machine image file shall use appropriate controls to protect the data at rest.

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

## SC-29 – Heterogeneity (Optional)

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

## SC-30 – Concealment and Misdirection (Optional)

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

## SC-31 – Covert Channel Analysis (Optional)

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

## SC-32 –System Partitioning (Optional)

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

## SC-33 – Transmission Preparation Integrity

[Withdrawn: Incorporated into SC-8].

## SC-34 – Non-Modifiable Executable Programs (Optional)

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

## SC-35 – External Malicious Code Identification (Optional)

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

## SC-36 – Distributed Processing and Storage (Optional)

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

## SC-37 – Out-of-Band Channels (Optional)

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

## SC-38 – Operations Security (Optional)

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

## SC-39 – Process Isolation (Optional)

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

## SC-40 – Wireless Link Protection

The confidentiality of data transmitted on external and internal wireless links shall be protected from corruption or data loss by doing the following.

a. Extending, modifying, or retransmitting network services, such as through the installation of new switches or wireless access points, is prohibited, unless prior approval is granted.

b. Wireless networks shall be physically or logically segregated from internal wired networks such that an unknown external user cannot access an organization's internal network.

c. All Restricted and Highly Restricted data shall be encrypted when transmitted across wireless or public networks, including transmissions such as SFTP and electronic mail. For the encryption requirements of secure transmission of confidential data, refer to SC-13 Cryptographic Protection.

d. All network access points shall be identified and safeguards for the network and individual systems shall be verified as adequate and operational. These systems include wireless access points, network ingress and egress points, and network-attached devices.

e. Use access points that require a key, and which encrypt the wireless communication.

f. Configure wireless LAN settings to not allow automatic joining of any wireless network.

g. For wireless LAN communications, the following encryption settings shall be used:

   i. Depending on the type of information traversing a wireless LAN, encryption is required at varying levels. At a minimum, public information requires Wi-Fi Protected Access (WPA) encryption and Restricted and Highly Restricted data require 802.11i (WPA2)-compliant Advanced Encryption Standard (AES) encryption. End-to-end encryption is highly recommended for the Restricted and Highly Restricted data classification.

   ii. If the Temporal Key Integrity Protocol (TKIP) is the highest level of encryption available for WPA, then WPA2 shall be used.

   iii. When WPA2 is used, AES encryption shall be enabled and shall be no less than 256 bits.

   iv. WPA2 (802.11i) encryption must use TKIP, Counter Mode CBC-MAC Protocol (CCMP), or other IEEE- or NIST-approved key exchange mechanism.

h. When end-to-end encryption is required across both an 802.11 wireless and a wired network, then in addition to WPA2 (802.11i), data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality. Such protocols include TLS, SSH, IP Security (IPSec) and VPN tunnels.

## SC-41 – Port and I/O Device Access (Optional)

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

## SC-42 – Sensor Capability and Data (Optional)

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

## SC-43 – Usage Restrictions

Organizations shall do the following regarding usage restrictions:

a. Establish usage restrictions and implementation guidance for information system components including, for example: hardware, software, or firmware components (e.g., VOIP, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).

b. Define the proper use of information assets through Acceptable User Policies (AUPs) and include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage and Internet usage. See the Statewide AUP for further guidance.

## SC-44 – Detonation Chambers

Organizations tasked with conducting incident response and forensics, should employ a detonation chamber capability also known as dynamic execution environments in a secure, quarantined environment, to do the following:

a. Allow the opening of email attachments.

b. Allow the execution of untrusted or suspicious applications.

c. Allow the execution of Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox to quickly identify malicious code.

d. Reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely).

e. This control is optional for LOW 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.

## 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 deployment, operation and maintenance of information systems and supporting infrastructure are responsible for adhering to this policy and with any local system and information integrity 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 is assigned the responsibility for documenting, disseminating and implementing the system and information integrity program throughout the agencies. |
| **Agency Security Liaison** | The Agency Security liaison is responsible for ensuring that information system and integrity requirements are managed in compliance with the State's requirements by collaborating with organizational entities.<br>Liaisons are responsible for maintaining the appropriate information system and communications protection required for information security protection. |
| **Information System Owner** | The Information System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |
| **Third Parties** | Third party service providers are responsible for ensuring that systems, system components and services they provide are secure and do not negatively impact security of pre-existing |

| | |
|---|---|
| | systems by implementing secure system and information integrity controls in accordance with this policy. |

## SI-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 NIST SP 800-53, Security and Privacy Controls. This document addresses the standards set forth by the State to implement the family of System and Information Integrity security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the System and Information Integrity principles established in NIST SP 800-53, "System and Information Integrity" control guidelines as the official policy for this security domain. The "SI" designator identified in each control represents the NIST-specified identifier for the System and Information Integrity control family. The following subsections in this document outline the System and Information Integrity requirements that each agency shall implement and maintain in order to protect the confidentiality, integrity and availability of information and information systems by assuring systems, system components and services acquired are secure and do not negatively impact security of pre-existing systems used for conducting the agencies' mission critical business functions.

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.

## SI-2 – Flaw Remediation

An explicit and documented patching and vulnerability policy is required, as well as a systematic, accountable, and documented set of processes and procedures for flaw remediation. The following are required:

a. The patching and vulnerability policy shall specify techniques an agency will use to identify, report, and correct information system flaws and personnel who will be responsible for the process.

    i. An organization's patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches.

ii. A list of sources of information about security problems and software updates for the system and application software shall be developed and maintained, and those sources shall be monitored regularly.

iii. Where technically configurable, tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention (See http://cve.mitre.org) and that use the Open Vulnerability Assessment Language (OVAL) shall be used to test for the presence of vulnerabilities.

iv. Vulnerability definitions and signatures shall be updated and reviewed prior to each scan or when new vulnerabilities are identified or reported.

v. Relevant vulnerability information from appropriate vendors, third party research, and public domain resources shall be reviewed on a regular basis, per the organization's policies and procedures.

vi. Relevant vulnerability information, as discovered, shall be distributed to the appropriate agency employees.

vii. System and application bug fixes or patches shall be accepted only from highly reliable sources, such as the software vendor.

viii. Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources.

ix. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available (zero-day vulnerability). When a vulnerability risk is "critical" or "high-level" and no patch is available, steps must be taken to mitigate the risk through other methods (e.g., workarounds, firewalls, router access control lists). A patch needs to be applied when it becomes available.

x. When a "critical" or "high-level" risk vulnerability cannot be totally mitigated within the requisite time frame, agencies need to notify agency management and the State Chief Information Security Officer (SCISO) of the condition and remediation plan and execution of a plan.

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

c. Install security-relevant software and firmware updates based on severity and associated risk. Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

d. Incorporate flaw remediation into the agency configuration management process.

e. Centrally managed and automated mechanisms shall be employed to determine the state of information system components about flaw remediation.

## Vulnerability Risk Ratings and Remediation

Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 "Qualitative Severity Rating Scale" for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a CVE, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above "info", or a score of 0, may be used after appropriate review.

The risk ratings and remediation timelines are assigned to a vulnerability as follows:

a. **Critical-level Risk** (Priority/CVSS 9.0-10.0)**:** A vulnerability that could cause grave consequences and potentially lead to leakage of sensitive data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, as identified by the data owner. Critical-level risk vulnerabilities must be, at a minimum, remediated within seven (7) days.

b. **High-level Risk** (Priority/CVSS 7.0-8.9)**:** A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. High-level risk vulnerabilities must be mitigated or remediated within thirty (30) days.

c. **Medium-level Risk** (Priority/CVSS 4.0-6.9)**:** A vulnerability that should be addressed within the established timelines. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner. Medium-level risk vulnerabilities must be mitigated or remediated within sixty (60) days.

d. **Low-level Risk** (Priority/CVSS 0.1-3.9)**:** A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Low-level risk vulnerabilities must be mitigated or remediated within ninety (90) days.

# SI-2 (2) – Flaw Remediation | Automated Flaw Remediation Status

Organizations shall determine per their defined frequency if system components have applicable security-relevant software and firmware updates installed using an agency-defined automated mechanism.

This control is optional for LOW risk information systems.

## SI-3 – Malicious Code Protection

Layers of information security (defense in depth) shall be implemented to defend against attacks on information resources, including malicious code protection, such as antivirus software and antimalware and intrusion detection systems. As applicable, malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles. The following shall be done:

a. Implement signature based and non-signature based malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

b. Automatically update malicious code protection mechanisms whenever new releases are available in accordance with agency configuration management policy and procedures.

c. Configure malicious code protection mechanisms to do the following:

   i. When using signature-based protection, conduct weekly periodic scans of the system.

   ii. When using signature based or non-signature-based protection, conduct real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency policy.

   iii. Block or quarantine malicious code and send an alert to an organizational defined role in response to malicious code detection.

   iv. Allow users to manually perform scans on their workstation and removable media.

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

e. Centrally manage malicious code protection mechanisms with automatic updates. Malicious code protection mechanisms include, for example, signature definitions. Updates shall be tested and approved according to the State's Configuration Management Policy, SCIO-SEC-305.

f. Ensure currently supported and patched software is installed to mitigate vulnerabilities and to reduce the risk of malicious activity.

g. Implement measures to filter unwanted traffic (spam, bots, etc.) attempting to enter the internal network.

h. Updates to virus scanning software and firewall systems shall be made available to users.

i. All files downloaded from a source external to the State Network, including all data received on a diskette, compact disc (CD), USB flash drive, email attachments, or any other electronic medium, shall come from a known, trusted source and shall be scanned for malicious software such as viruses, Trojan horses, worms, or other destructive code. This includes files obtained through any other file transfer mechanism.

j. Web browser software shall be properly configured to protect the State's information technology systems. Configuration requirements for Web browser software may be found in the Configuration Management Policy, SCIO-SEC-305, Section CM-6.

## SI-4 – System Monitoring

A program for continuous monitoring and auditing of system use shall be implemented to detect unauthorized activity. This includes systems that are cloud hosted by contracted vendors or agency managed.

a. Information systems shall be monitored to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections.

b. Organizations shall identify unauthorized use of the information system:

   i. All hardware connected to the State Network or is cloud hosted shall be configured to support State/agency management and monitoring standards.

   ii. Monitoring for attempts to deny service or degrade the performance of information systems.

   iii. Conducting periodic reviews of system logs for signs of misuse, abuse, or attack.

c. Internal monitoring capabilities or monitoring devices and controls shall be used to help secure the State's resources. These controls shall include the following:

   i. Securing interfaces between agency-controlled and non-agency-controlled or public networks.

   ii. Standardizing authentication mechanisms in place for both users and equipment.

   iii. Appropriate user access controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task.

   iv. Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date.

   v. Analyze detected events and anomalies.

d. The level of system monitoring of activity shall be adjusted when there is a change in risk to the organization's operations and assets, individuals, other organizations, or the State.

e. Provide information system monitoring information to designated agency officials as needed.

f. Agencies shall obtain legal opinion about information system monitoring activities.

## SI-4 (2) – System Monitoring | Automated Tools for Real-Time Analyses

Automated tools shall be employed to support near real-time analysis of events. Automated tools include, for example, host-based, network-based, transport-based, or storage-based event

monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by agency information systems.

This control is optional for LOW risk information systems.

## SI-4 (4) – System Monitoring | Inbound and Outbound Communications Traffic

a. The criteria for unusual or unauthorized activities or conditions shall be determined for inbound and outbound communications traffic

b. Inbound and outbound communications traffic shall be monitored for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within agency information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

c. Logging features on firewalls, (network and web application firewalls (WAF)), shall be enabled to capture all packets dropped or denied by the firewall. Those logs shall be reviewed at least monthly.

d. Firewall policies shall be reviewed and verified at least quarterly. If an outside entity, such as DIT, manages the firewall, then that entity shall be responsible for providing the agency's firewall policy to the responsible agency for review and corrective actions, at minimum quarterly.

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

## SI-4 (5) – System Monitoring | System Generated Alerts

a. Information systems shall alert authorized personnel, such as system administrators, mission/business owners, system owners, or information system security officers, when system-generated indications of compromise, potential compromise, or detected suspicious events occur. Necessary actions shall be taken to address suspicious events once detected.

b. Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, web Application Firewalls (WAF), or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, by telephone, electronic mail messages, or text messages.

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

## SI-5 – Security Alerts, Advisories, and Directives

Organizations shall do the following:

a. Receive information system security alerts, advisories, and directives from external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations on an ongoing basis.

b. Generate internal security alerts, advisories, and directives as deemed necessary.

c. Disseminate security alerts, advisories, and directives to designated organizational management and technical staff as appropriate.

d. Implement security directives in accordance with established time frames or notifies the issuing agency of the degree of noncompliance.

e. Take appropriate actions in response to security alerts/advisories.

   i. Any updates or notices from the ESRMO must be implemented per change control and/or incident response procedures.

   ii. The ESRMO must be contacted with any security alert/advisory concerns or must be notified when the actions are completed.

The ESRMO shall maintain contact with special interest groups (e.g., information security forums) that does the following:

   i. Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies)

   ii. Provide access to advice from security professionals

   iii. Improve knowledge of security best practices

## SI-6 – Security and Privacy Function Verification (Optional)

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

## SI-7 – Software, Firmware, and Information Integrity

Integrity verification tools shall be employed to detect unauthorized changes to software, firmware, and information.

a. Error logs generated by information technology systems shall be regularly monitored and reviewed for abnormalities and shall be:

i. Cross-checked for known security events based on network, size, system type and logical and physical location.

ii. Enabled on each device or system on the network, such as servers, firewalls, routers, switches, cache engines, intrusion detection systems (IDSs) and applications, if performance requirements are not affected.

iii. Monitored on a weekly basis at a minimum.

iv. Checked against baselines to effectively verify variations from normal work-related activities.

b. Documentation and appropriate actions need to be taken for the detection of the unauthorized change, so that they are integrated into the incident response capability and such events are tracked, corrected and available for historical purposes. When unauthorized changes to the software, firmware and information are detected, the following actions should be taken:

i. Alert authorized personnel of any unauthorized changes (e.g., using an integrity verification tool) and send the alert to a SIEM (if available) to incorporate it into the incident response process.

ii. Ensure help desk/support tickets get opened using identified tools/mechanisms to ensure tracking and closure for those incidents.

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

## SI-7 (1) – Software, Firmware, and Information Integrity – Integrity Checks

a. Information systems shall perform an integrity check of organizational-defined software, firmware, and information at transitional states, such as, system startup, restart, shutdown, and abort, as well as when any security-relevant events occur. Security-relevant events include, for example, the identification of a new threat to which information systems are susceptible, and the installation of new hardware, software, or firmware.

b. The integrity of backup or image files shall be validated using file hashes for backups, restores, and virtual machine migrations.

c. After making any changes in a system's configuration or its information content, new cryptographic checksums or other integrity-checking baseline information shall be created for the system.

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

## SI-7 (7) – Software, Firmware, and Information Integrity – Integration of Detection and Response

The detection of security-relevant changes to information systems shall be incorporated into the organization's incident response capability. This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes.

Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

This control is optional for LOW risk information systems.

## SI-8 – Spam Protection

Organizations shall do the following to protect resources from electronic mail (email) threats:

a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited email messages (spam).

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

c. Protect State resources by not taking action on unsolicited commercial electronic mail. Recipients shall not open or respond to unsolicited email.

d. Educate users on the potential security risks involved in responding to spam, including responding to an invitation contained in such email to have one's email address removed from a sender's list.

e. Establish procedures that address the following issues:

   i. Attacks on email (e.g., viruses, interception, user identification, defensive systems).

   i. Activating or clicking on hyperlinks in documents or email messages that are from unknown sources or part of unsolicited messages.

   ii. Responding to or following hyperlinks asking for usernames and passwords when asked to do so by unsolicited phishing emails.

   iii. Protection of electronic mail attachments using such techniques as filtering, stripping and store and forward.

   iv. Use of cryptography to protect the confidentiality and integrity of electronic messages.

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

## SI-8 (1) – Spam Protection – Central Management (Moderate Control)

Spam protection mechanisms shall be centrally managed. Central management is the organizational-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.

This control is optional for LOW risk information systems.

## SI-8 (2) – Spam Protection – Automatic Updates

Spam mechanisms shall be automatically updated regularly on an organizational-defined frequency.

This control is optional for LOW risk information systems.

## SI-9 – Information Input Restrictions

Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6

## SI-10 – Information Input Validation

Information systems shall check the validity of information inputs by doing the following:

a. Rule check the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) required to execute job functions.

b. Prescreen and validate inputs prior to passing to interpreters to prevent the content from being unintentionally interpreted as commands.

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

## SI-11 – Error Handling

Information systems shall do the following:

a. Generate error messages that provide information necessary for corrective actions without revealing information, including, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers that could be exploited.

b. Reveal error messages only to designated agency personnel.

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

## SI-12 – Information Management and Retention

Information within a system and information output from a system shall be managed and retained in accordance with applicable federal laws, directives, policies, regulations, State standards, and operational requirements.

Forwarding and auto-forwarding of state data must comply the Statewide Acceptable Use Policy (AUP). Policies shall be developed to encourage due care by users when forwarding electronic messages so that users do not do the following:

a. Knowingly send out an email message that contains viruses, Trojan horses, or other malware.

b. Use the electronic-mail system or network resources to propagate chain letters, misinformation, or hoax information.

c. Forward any Restricted or Highly Restricted information to any unauthorized party without prior management approval, and without appropriate protections, such as encryption.

d. Forward the wrong attachment.

e. Send information or files that can cause damage to the State of North Carolina or its citizens.

f. Send unsolicited messages to large groups of people except as required to conduct agency business.

Communications sent or received by email systems and/or email communications on State business in personal email accounts may be public records as defined by the North Carolina Public Records Law, N.C.G.S. §132.1, *et seq.,* and shall be managed according to the requirements of an agency's record retention policy or as set forth in the General Schedule for Electronic Records published by the Department of Cultural and Natural Resources.

## SI-13 – Predictable Failure Prevention (Optional)

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

## SI-14 – Non-Persistence (Optional)

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

## SI-15 – Information Output Filtering (Optional)

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

## SI-16 – Memory Protection

Security safeguards shall be implemented to protect the volatile memory of information systems from unauthorized code execution.

a. Data execution prevention and address space layout randomization shall be implemented. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

b. The integrity and stability of the State Network shall be protected from fraudulent use and/or abuse resulting from access and use of the network. The security attributes delivered with network services shall be defined.

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

## SI-17 – Fail-Safe Procedures (Optional)

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.

## Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. They 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, and other policies, standards, and guidelines.

This policy provides the State of North Carolina's (State) Supply Chain Risk Management policy statements and commitment to develop, implement, maintain reasonable supply chain assurance methods and practices to strategically manage supply chain risks over the life cycle of information systems, products, and services.

## 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 that are included in IT risk assessment activities are responsible for adhering to this policy and with any local Risk Assessment requirements.

| Role | Definition |
|---|---|
| **Senior Management** | Senior Management (the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designating organizational official) is responsible for the sponsorship and support of the Supply Chain Risk Management Plan and process, the review and approval of risk assessments and control recommendations and reporting to the SCRO what mitigation actions have been taken. |
| **State Chief Information Security Officer** | The State Chief Information Security Officer (SCISO) as delegated by the State CIO is assigned the responsibility for the continued development, implementation, and maintenance of the risk management program. |

| | |
|---|---|
| **Risk Management** | The Enterprise Security and Risk Management Office (ESRMO) is responsible for governing the overall Security and Risk Management process, reviews presented Risk Assessment Reports and approves risk treatment plans or recommended controls. |
| **Security Liaison** | Security Liaisons are responsible for ensuring risk assessments are conducted, analyzing the risk and recommends controls, presenting risks for approval, documenting the process, and managing and facilitating the implementation of recommended controls. |
| **System Owner / Administrator** | System Owners/Administrators are responsible for participating in the identification and analysis process, participating in the risk identification and analysis process, and for the implementation of technical controls. |
| **Functional Managers** | Managers in the functional areas are responsible for participating in the risk identification and analysis process, and for the implementation of administrative controls. |

## SR-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 Supply Chain Risk Management security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the Supply Chain Risk Management security principles established in NIST SP 800-53, "Supply Chain Risk Management" control guidelines as the official policy for this security domain. The "SR" designator identified in each control represents the NIST-specified identifier for the Supply Chain Risk Management control family. The following subsections in this document outline the Supply Chain Risk Management requirements that each agency shall implement and maintain to manage risks that touch sourcing, vendor management, and supply chain quality across State agencies.

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.

## SR -2 – Supply Chain Risk Management Plan

The following shall be implemented:

a. Develop a plan for managing supply chain risks associated with acquisition, delivery, integration, operations and maintenance, and disposal of the information systems and services:

   i The Supply Chain Risk Management (SCRM) plan should provide the basis for determining whether a technology, service or information system is fit for purpose and as such the controls need to be tailored accordingly.

   ii The SCRM plan shall include the following:

      1. an expression of the supply chain risk tolerance for the agency;
      2. acceptable supply chain risk mitigation strategies or controls;
      3. a process for consistently evaluating and monitoring supply chain risk;
      4. approaches for implementing and communicating the plan;
      5. a description of and justification for supply chain risk mitigation measures taken; and associated roles and responsibilities.

b. Review and update the supply chain risk management plan on an annual basis or as required, to address threat, organizational or environmental changes.

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

## SR-2 (1) – Supply Chain Risk Management Plan | Establish SCRM Team

The following shall be implemented:

a. Establish a supply chain risk management team that consists of the agency-defined roles and is responsible for identifying, assessing, and managing risks while using coordinated efforts.

b. The SCRM team shall consist of personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executives, information technology, contracting, information security, privacy, mission, or business, legal, supply chain and logistics and acquisition.

c. The SCRM team shall be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

## SR-3 – Supply Chain Controls and Processes

The following shall be implemented:

a. Establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems in coordination with the identified supply chain personnel.

i Supply chain elements include organizations, entities, or tools employed for the acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components.

ii Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

b. Employ the following controls to protect against supply chain risks to information assets, systems, system components, or system services and to limit the harm or consequences from supply chain-related events (examples):

i Control Assessments (CA-2)
ii External System Services (SA-9)
iii Acquisition Process (SA-4)
iv Controlled Maintenance (MA-2)
v Component Authenticity (SR-11)
vi Component Disposal (SR-12)

c. Document the selected and implemented supply chain processes and controls in an agency-defined document such as a SCRM plan.

## SR-5 – Acquisition Strategies, Tools, and Methods

Acquisition strategies, contract tools, and procurement methods shall be employed to protect against, identify, and mitigate supply chain risks. Examples are as follows:

a. Including incentive programs to system integrators, suppliers, or external services providers to ensure that they provide verification of integrity as well as traceability.

b. Requiring tamper-evident packaging.

c. Using trusted or controlled distribution.

## SR-6 – Supplier Assessments and Reviews

Supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide shall be assessed and reviewed annually.
An assessment and review of supplier risk should include security and supply chain risk management processes, foreign ownership, and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

The reviews shall consider documented processes, documented controls, and publicly available information related to the supplier or contractor.

This control is optional for LOW risk information systems.

## SR-8 – Notification Agreements

Agreements and procedures with entities involved in the supply chain shall be established for the notification of supply chain compromises including security incident and a privacy breach and the notification of assessment or audit results.

## SR-10 – Inspection of Systems or Components

A process to inspect information systems annually or upon any indications of the tampering of information systems shall be implemented.

Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

## SR-11 – Component Authenticity

The following shall be implemented:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to the agency-defined personnel.

Organizations should include in their anti-counterfeit policy and procedures, a means to help ensure that the components acquired and used are authentic and have not been subject to tampering.

## SR -11 (1) – Component Authenticity | Anti-Counterfeit Training

The following agency-defined roles shall be trained to detect counterfeit system components (including hardware, software, and firmware).

a. Personnel conducting configuration management activities
b. System administrators
c. Database administrators
d. Network administrators
e. Procurement personnel

## SR-11 (2) – Component Authenticity | Configuration Control for Component Service and Repair

Configuration control shall be maintained over system components awaiting service or repair and serviced or repaired components awaiting return to service.
Organizations shall manage risks associated with component repair including the repair process and any replacements, updates, and revisions of hardware and software components within the supply chain infrastructure.

## SR-12 – Component Disposal

Defined data, documentation, tools, or system components shall be disposed of without exposing sensitive or operational information, which may lead to a future supply chain compromise. Examples include the following:

a. Monitoring and documenting the chain of custody through the destruction process.

b. Training disposal service personnel to ensure accurate delivery of service against disposal policy and procedures.

c. Implementing assessment procedures for the verification of disposal processes with a frequency that fits agency needs.

d. Using Media Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

## 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.