

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
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.

Material Superseded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. 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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4
		Page No. 2 of 11

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:

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309	
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4	Page No. 3 of 11

- 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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4
		Page No. 4 of 11

- 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

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4
		Page No. 5 of 11

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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309	
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4	Page No. 6 of 11

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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4
		Page No. 7 of 11

- 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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4
		Page No. 8 of 11

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:

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4
		Page No. 9 of 11

- 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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309	
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4	Page No. 10 of 11

- 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.

	<h1>Maintenance Policy</h1>	Document No. SCIO-SEC-309	
Effective Date 01/29/2018	Review Date 03/26/2025	Version 4	Page No. 11 of 11

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.