Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

Responsibilities

All covered personnel 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 and implementing system and information integrity practices 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. Liaisons are responsible for maintaining the appropriate that 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 by assuring 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

All agency information assets must meet the required security controls defined in the NIST SP 800-53, Rev 4, Security and Privacy Controls. This document addresses the procedures and standards set forth by the State to implement the family of System and Information Integrity security controls.

The State has adopted the System and Information Integrity principles established in NIST SP 800-53 Rev 4, "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 shall be reviewed annually, at a minimum.

SI-2 – Flaw Remediation

Agencies shall have an explicit and documented patching and vulnerability policy, as well as a systematic, accountable, and documented set of processes and procedures for flaw remediation. Agencies must do the following:

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 agency'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. Agencies shall develop and maintain a list of sources of information about security problems and software updates for the system and application software and monitor those sources regularly.

   iii. Agencies shall use where possible 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) to test for the presence of vulnerabilities.

   iv. Agencies shall update and review vulnerability definitions and signatures 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 agency'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 Risk Officer (SCRO) 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. Agencies shall employ a centrally managed and automated mechanisms to determine the state of information system components about flaw remediation.

Vulnerability Risk Ratings and Remediation

The risk ratings and remediation timelines are assigned to a vulnerability are as follows:

a. **Critical-level Risk:** 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:** 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:** 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:** 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-3 – Malicious Code Protection

Agencies shall implement layers of information security (defense in depth) to defend against attacks on the State's 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. Agency shall do the following:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

b. 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. Perform periodic scans of the information system weekly and 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 security policy.

   ii. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection.

   iii. 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 information 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. The agency shall ensure that updates to virus scanning software and firewall systems are 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. Agencies shall ensure that Web browser software is 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 - Information System Monitoring

Agencies shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity.

a. Agencies shall monitor information systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections.

b. Agencies shall identify unauthorized use of the information system:

   i. All hardware connected to the State Network or agency network 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. Agencies shall deploy monitoring devices and controls to ensure that the State's 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. 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.

d. Agencies shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to agency operations and assets, individuals, other organizations, or the State based on law enforcement information, intelligence information, or other credible sources of information.

e. Provide information system monitoring information to designated agency officials as needed.

f. Agencies shall obtain legal opinion about information system monitoring activities in accordance with applicable federal laws, directives, policies, or regulations.

SI-4 (2) - Information System Monitoring – Automated Tools for Real-Time Analyses (Moderate Control)

Agencies shall employ automated tools 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.

SI-4 (4) - Information System Monitoring – Inbound and Outbound Communications Traffic (Moderate Control)

a. Agencies shall monitor inbound and outbound communications traffic 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.

b. Agencies shall enable logging features on state network firewalls to 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.

c. Agencies shall review and verify their firewall policies at least quarterly. If an outside entity, such as DIT, manages the firewall, then that entity shall be responsible for reviewing and verifying the agency's firewall policy at least quarterly.

SI-4 (5) - Information System Monitoring – System Generated Alerts (Moderate Control)

a. Agency information systems shall alert authorized personnel, such as system administrators, mission/business owners, system owners, or information system security officers, when indications of compromise, potential compromise, or detected suspicious events occur. Agencies shall take necessary actions 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, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, by telephone, electronic mail messages, or text messages.

SI-5 – Security Alerts, Advisories, and Directives

Agencies 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 agency 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 agency 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 Function Verification (Optional)

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

SI-7 – Software, Firmware, and Information Integrity

Agencies shall employ integrity verification tools to detect unauthorized changes to agency 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. This control is optional for LOW risk information systems.

SI-7 (1) – Software, Firmware, and Information Integrity – Integrity Checks (Moderate Control)

a. Agency information systems shall perform an integrity check of agency-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 agency 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, agencies shall create new cryptographic checksums or other integrity-checking baseline information for the system.

SI-7 (7) – Software, Firmware, and Information Integrity – Integration of Detection and Response (Moderate Control)

Agencies shall incorporate the detection of unauthorized changes security-relevant changes to information systems into the agency 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.

SI-8 – Spam Protection

Agencies shall do the following to protect State 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. Develop policies to encourage due care by users when forwarding messages so that users do not do the following:

   i. Auto-forward email without first obtaining agency approval.

   ii. Knowingly send out an email message that contains viruses, Trojan horses or other malware.

   iii. Use the electronic-mail system or network resources to propagate chain letters, misinformation or hoax information.

   iv. Forward any restricted or highly restricted information to any unauthorized party without prior management approval, or without appropriate protections, such as encryption.

   v. Forward the wrong attachment.

   vi. Send information or files that can cause damage to the State of North Carolina or its citizens.

   vii. Send unsolicited messages to large groups of people except as required to conduct agency business.

f. 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 user names 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.

g. Communications sent or received by agency 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.

h. Agencies information systems shall automatically update spam protection mechanisms.

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

SI-8 (1) – Spam Protection – Central Management (Moderate Control)

Agencies shall centrally manage spam protection mechanisms. Central management is the agency-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.

SI-9 – Information Input Restrictions

Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6

SI-10 – Information Input Validation

Agency 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

Agency 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 by adversaries.

b. Reveal error messages only to designated agency personnel.

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

SI-12 – Information Handling and Retention

Agencies shall handle and retain information within an information system and information output from the system in accordance with applicable federal laws, directives, policies, regulations, State standards, and operational requirements.

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

Agencies shall implement security safeguards to protect the volatile memory of its information systems from unauthorized code execution.

a. Agencies shall implement data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

b. Agencies shall protect the integrity and ensure the stability of the State Network from fraudulent use and/or abuse resulting from access and use of the network and to define the security attributes delivered with network services.

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.

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

Secretary of Department of Information Technology (DIT)

Policy Approval and Review

Name	Reason	Date