GOVERNANCE

This document is governed by the IT Governance policy which provides the following requirements:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and systems used, managed, or operated by a contractor, 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 systems supporting the operation and assets of the State.

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls.

APPLICABILITY

This document addresses the requirements 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 and provides requirements for the System and Integration Integrity process to assure information systems are designed and configured using controls sufficient to safeguard the State's systems and data.

SI-1 POLICY AND PROCEDURES

The State has adopted the System and Information Integrity principles established in NIST SP 800-53 r5, "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. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections outline the System and Information Integrity requirements the State and executive-branch agencies must implement and maintain for policy compliance.

This policy and associated procedures shall be reviewed and updated at least every three (3) years unless State-defined events require more frequent review.

The requirements of the System and Information Integrity policy are the following:

Develop, document, and disseminate to all State employees, contractors, agencies, or other organizations on behalf of the State a policy that:

a. Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
c. States procedures to facilitate the implementation of the System and Information Integrity policy and the associated System and Information Integrity controls.
d. Designates an official to manage the development, documentation, and dissemination of the System and Information Integrity policy and procedures.

The System and Information Integrity Policy shall be reviewed at least every three (3) years or as agency-defined events require.

SI-2 FLAW REMEDIATION

The State and executive-branch agencies, contractors, or other organizations acting on behalf of the State shall identify, report, and correct information system security flaws discovered when accessing State information resources.

Organizations shall have a patching process defining a method for deciding which systems are patched and when patches are installed, and the method for testing and safely installing patches.

a. A list of sources of information about security problems and software updates for systems and application software shall be developed and maintained, and those sources shall be monitored regularly.
b. Where technically configurable, vulnerability scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention (See http://cve.mitre.org) shall be used to test for vulnerabilities.
c. Vulnerability definitions and signatures shall be updated and reviewed prior to each scan or when new vulnerabilities are identified or reported.
d. 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.
e. Relevant vulnerability information shall be distributed to the appropriate agency employees.
f. System and application bug fixes or patches shall be accepted only from highly reliable sources, such as the software vendor.
g. Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources.
h. 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, etc.). A patch must be applied when it becomes available.
i. When a “critical” or “high-level” risk vulnerability cannot be mitigated within the requisite time frame, agencies should notify agency management and the Information Security Officer of the condition and[GM1] remediation plan and execution of a plan.
j. Software and firmware updates related to flaw remediation must be tested for effectiveness and

potential side effects before installation.

k. Security-relevant software and firmware updates are installed based on severity and associated risk. Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

l. Flaw remediation is incorporated into the organizational configuration management process.

m. Centrally managed and automated mechanisms shall be employed to determine the state of information system components about flaw remediation.

n. Where technically possible, 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.

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

   i. 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.

   ii. 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.

   iii. 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.

   iv. 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 or can be remediated via an approved exception.

SI-2 (2) FLAW REMEDIATION - AUTOMATED FLAW REMEDIATION STATUS

Determine if system components can have applicable security-relevant software and firmware updates installed using an agency-defined automated mechanism.

SI-3 MALICIOUS CODE PROTECTION

The following shall be performed:

a. Implement signature-based and non-signature-based malicious code protection mechanisms at system network entry and exit points to detect and eradicate malicious code.
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.
c. Configure malicious code protection mechanisms to:
    i. Perform periodic weekly scans of systems and real-time scans of files from external sources at endpoint, network entry, and exit points as the files are downloaded, opened, or executed in accordance with organizational policy.
    ii. Block or quarantine malicious code and send an alert to organization-defined personnel to investigate and respond to the malicious code detection.
d. Address the receipt of false positives during malicious code detection to prevent potential impact on system availability.
e. Centrally manage malicious code protection mechanisms with automatic updates. Not less than daily, the agency shall check for updates to malicious code scanning tools, including anti-virus (AV), anti-spyware software, and intrusion detection tools. When updates are available, immediately implement them on all devices on which such tools reside.
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 malicious network traffic (spam, bots, etc.) attempting to enter State networks.

SI-4 SYSTEM MONITORING

Systems, networks, and cloud environments shall be monitored to detect:

a. Attacks and indicators of potential attacks;
b. Unauthorized access; and
c. Unauthorized local and remote connections.

The State and executive-branch agencies shall identify unauthorized use of systems by conducting periodic reviews of system, network, or cloud environment logs for signs of misuse, abuse, or attack, and strategically deploy event and anomaly detection monitoring to collect essential events. Ad hoc monitoring also may be specified at certain system points to tactically track specific transition types of interest to the agency.

The following shall also be performed:

a. Analyze detected events and anomalies to determine if a security incident has occurred.
b. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the State.
c. Obtain legal opinion regarding system monitoring activities.
d. Provide information system monitoring events to designated agency officials as needed.

SI-4 (2) SYSTEM MONITORING – AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Automated tools shall be employed to support near real-time analysis of events and include but are not limited to host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies for real-time alert analysis and notifications generated by agency information systems.

SI-4 (4) SYSTEM MONITORING – INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

The State and executive-branch agencies shall determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic and subsequently monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions such as:

a. Internal traffic that indicates the presence of malicious code within agency information systems or propagating among system components;
b. The unauthorized exporting of information; and
c. Malicious connections to external systems.

Firewall policies shall be reviewed and verified at least quarterly. If an outside entity manages the firewall, then that entity is responsible for providing the agency's firewall policy to the responsible agency for review and corrective actions at least quarterly.

SI-4 (5) SYSTEM MONITORING – SYSTEM-GENERATED ALERTS

Information systems shall alert authorized personnel, such as system administrators, business owners, system owners, or information system security officers, when system generated indications of compromise or potential compromise events occur. Necessary actions shall be taken to address suspicious events when detected per the Incident Response policy.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

The State and Executive Branch agencies shall:

a. Receive system security alerts, advisories, and directives from the Cybersecurity and Infrastructure Security Agency (CISA) and State-utilized vendors 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 notify the issuing organization of the degree of noncompliance; and
e. Take appropriate actions in response to security alerts and/or advisories.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Integrity verification tools shall be used to detect unauthorized changes to organizational-defined software, firmware, and information.

The following actions shall be taken when unauthorized changes to the software, firmware, and information are detected:

a. Check against baselines to effectively verify variations from normal work-related activities;
b. Document any appropriate actions needed to be taken for the detection of the unauthorized change;
c. Alert authorized personnel of any unauthorized changes so that it is incorporated into the

incident response process; and

d. Ensure a security incident is opened to ensure tracking and remediation of the reported incident.

SI-7 (1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY – INTEGRITY CHECKS

Integrity checks shall be performed on organization-defined software, firmware, and information at transitional states, such as, system startup, restart, shutdown, abort, and when any security-relevant events occur.

The integrity of backup or image files shall be validated using file hashes for backups, restores, and virtual machine migrations.

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.

SI-7 (7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY – INTEGRATION OF DETECTION AND RESPONSE

The State and executive-branch agencies shall incorporate any detection of unauthorized changes to established configuration settings or the unauthorized elevation of system privileges into the incident response process. Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions.

SI-8 SPAM PROTECTION

Spam protection mechanisms shall be employed at system entry and exit points to detect and act on unsolicited messages. Spam protection mechanisms shall also be updated when new releases are available as stated by organizational configuration management policies and procedures.

State resources shall be protected by not acting on unsolicited electronic mail. Recipients shall not respond to unsolicited email.

Procedures and training shall be established to address:

a. Attacks on email (e.g., viruses, interception, user identification, defensive systems)
b. Activating or clicking on hyperlinks in documents or email messages that are from unknown sources or part of unsolicited messages.
c. Responding to or following hyperlinks asking for usernames and passwords when asked to do so by unsolicited phishing emails.
d. Protection of electronic mail attachments using techniques such as filtering, stripping, and store and forward.
e. Use of cryptography to protect the confidentiality and integrity of electronic messages.

SI-10 INFORMATION INPUT VALIDATION

Information systems shall:

a. 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.

SI-11 ERROR HANDLING

Information systems shall:

a. Generate error messages that provide information necessary for corrective actions without revealing 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.

SI-12 INFORMATION MANAGEMENT AND RETENTION

Information shall be managed and retained within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

SI-16 MEMORY PROTECTION

Security safeguards shall be implemented to protect the volatile memory of information systems from unauthorized code execution.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED [Policy Updates]

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK