Division of Enterprise Technology Strategy and Services

ETSS Policy 300.5

System and Information Integrity Policy (SI)

Publish Date: 15 July 2026
Effective Date: 15 July 2026
Last Revision Date: 14 July 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for maintaining the integrity of State of Rhode Island information systems and data. It defines controls for flaw remediation, malicious code protection, system monitoring, security alerts, software and firmware integrity verification, spam protection, information input validation, error handling, information retention, and memory protection. These controls work together to detect, prevent, and respond to threats that could compromise the confidentiality, integrity, or availability of State information systems and data.
This policy supports the State's compliance with NIST SP 800-53 Revision 5 (System and Information Integrity family), NIST SP 800-40 (Enterprise Patch Management), NIST SP 800-83 (Malware Incident Prevention), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For the purposes of this policy, the term "Agency" refers to any department, agency, division, or unit of the Executive Branch.

3. Definitions

The following terms are defined for the purposes of this policy. All other terms should be referenced in the ETSS Glossary of Terms, Acronyms, and Definitions.

Malicious Code
Software or firmware intended to perform an unauthorized process that has an adverse impact on the confidentiality, integrity, or availability of an information system, such as a virus, worm, Trojan horse, spyware, ransomware, or other code-based entity that infects a host.

Flaw Remediation
The process of identifying, reporting, testing, and correcting security-relevant defects in information system software, firmware, or hardware, including the installation of patches, updates, and hot fixes.

Integrity Verification
The use of tools and techniques to detect unauthorized changes to software, firmware, and information, including file integrity monitoring, code signing, hash verification, and configuration baseline comparison.

4. Procedures for Compliance

The following requirements establish the system and information integrity controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1 System and Information Integrity Policy and Procedures (SI-1)

Applies to: All systems (IAL1, IAL2)
Each agency shall develop, document, and disseminate a system and information integrity policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The ETSS CISO is designated as the official responsible for the enterprise policy. The policy shall be reviewed and updated at least every three (3) years and following significant changes. Supporting procedures shall be reviewed in alignment with the policy.

4.2 Flaw Remediation (SI-2)

Applies to: All systems (IAL1, IAL2)
Each agency shall:

a. Identify, report, and correct information system flaws. See ETSS Risk Assessment (RA), ETSS Configuration Management (CM), and NIST SP 800-40 Rev. 4 (Enterprise Patch Management Planning) policies for guidance.

b. Test software and firmware updates related to flaw remediation for potential impacts prior to installation.

c. Install security-relevant software and firmware updates based on the criticality of the update and security category of the information system within the following timelines: critical findings within fifteen (15) days of identification; high findings within thirty (30) days; moderate findings within ninety (90) days; and low findings within one hundred eighty (180) days. Where remediation within these timelines is not feasible, a documented risk acceptance or Plan of Action and Milestones (POAM) is required.

d. Incorporate flaw remediation into the agency configuration management process.

4.2.1 Automated Flaw Remediation Status (SI-2(2))

Applies to: Moderate and above (IAL2)
Each agency shall employ automated mechanisms to determine, on at least a monthly basis, whether information system components have applicable security-relevant software and firmware updates installed. Remediation performance data shall be captured through enterprise vulnerability management and IT service management platforms and reported through the continuous monitoring program.

4.2.2 Time to Remediate Flaws and Benchmarks for Corrective Actions (SI-2(3))

Applies to: Moderate and above (IAL2)
Each agency shall:

a. Measure the time between flaw identification and flaw remediation.

b. Establish and adhere to the benchmarks for corrective actions defined in Section 4.2(c) of this policy. Benchmark compliance shall be tracked and reported through enterprise vulnerability management tools and the continuous monitoring program.

4.3 Malicious Code Protection (SI-3)

Applies to: All systems (IAL1, IAL2)

ETSS shall centrally manage malicious code protection mechanisms wherever possible. Where systems cannot be centrally managed by ETSS, the agency shall be responsible for planning, assessing, authorizing, implementing, and monitoring malicious code protection controls. Agencies shall adopt a defense-in-depth strategy integrating endpoint detection and response (EDR), firewalls, intrusion detection systems, email security, encryption, and strong authentication. Each agency shall:

a. Employ signature-based and non-signature-based (behavioral, machine learning) malicious code protection mechanisms at information system entry and exit points, including endpoints, network entry and exit points, email gateways, web proxies, and remote access servers, to detect and eradicate malicious code.

b. Automatically update malicious code protection mechanisms when new releases are available in accordance with ETSS configuration management policy and procedures. Updates shall be deployed from vendor cloud-based infrastructure without requiring manual intervention where feasible.

c. Configure malicious code protection mechanisms to: (1) perform near real-time endpoint protection and detection with at least monthly vulnerability scanning for all endpoints supporting constituent-facing systems; (2) perform real-time scans of files from external sources at endpoints and network entry/exit points as files are downloaded, opened, or executed; and (3) block and quarantine malicious code, generate alerts to security operations personnel, and initiate mitigation actions in accordance with the ETSS Incident Response Plan.

d. Address the receipt of false positives during malicious code detection and eradication, including a tiered detection approach where suspicious but unconfirmed detections are quarantined and reviewed before permanent action is taken. False positive determinations shall be documented and used to tune detection rules.

4.4 System Monitoring (SI-4)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Monitor information system activities and access patterns to detect: (1) attacks and indicators of potential attacks in accordance with the ETSS Incident Response Plan, including irregularities, anomalies, and other indicators of compromise; (2) unauthorized local, network, or remote connections, with appropriate actions taken to sever unauthorized connections; and (3) proper functioning of internal processes and controls.

b. Identify unauthorized use of the information system using methods defined in the applicable System Security Plan. See ETSS Audit and Accountability Policy (300.x) for additional guidance.

c. Deploy monitoring devices strategically within the information system to collect essential information, and at ad hoc locations to track specific types of transactions of interest.

d. Analyze detected events and anomalies. Enterprise monitoring tools shall correlate events from multiple sources to identify patterns, trends, and advanced persistent threats.

e. Protect information obtained from monitoring tools from unauthorized access, modification, and deletion.

f. Increase system monitoring activity when there is an indication of increased risk based on law enforcement information, threat intelligence, or other credible

sources.

g. Obtain a legal opinion regarding system monitoring activities to ensure compliance with applicable federal and State laws.

h. Provide system monitoring information to designated agency officials within the frequency defined in the System Security Plan.

4.4.1 Automated Tools and Mechanisms for Real-Time Analysis (SI-4(2))

Applies to: Moderate and above (IAL2)

Each agency shall employ automated tools to support near real-time analysis of events with information security implications. Enterprise Security Information and Event Management (SIEM) capabilities shall be leveraged for centralized, real-time monitoring of information system events, with alerting and correlation to support incident detection and response.

4.4.2 Inbound and Outbound Communications Traffic (SI-4(4))

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic, based on a documented baseline of normal communications.

b. Continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities, including large file transfers, persistent connections, unusual protocols and ports, and attempted communications with suspected malicious external addresses.

4.4.3 System-Generated Alerts (SI-4(5))

Applies to: Moderate and above (IAL2)

Each agency shall alert system administrators, business owners, system owners, system security officers, or other designated personnel when suspicious events and indicators of compromise are detected, including the presence of malicious code, unauthorized export of non-public data, unauthorized signaling to external systems, and potential intrusions. Alerts may be generated from audit records, malicious code protection mechanisms, intrusion detection or prevention mechanisms, endpoint detection and response tools, and boundary protection devices, and may be transmitted via automated alerting systems, email, or other approved notification methods.

4.5 Security Alerts, Advisories, and Directives (SI-5)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Receive information system security alerts, advisories, and directives from designated external agencies, mission-critical entities, and service providers 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 officials and external authorities as appropriate.

d. Implement security directives in accordance with established timeframes or notify the issuing entity of the degree of non-compliance.

4.6 Software, Firmware, and Information Integrity (SI-7)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information, including operating system kernels, drivers, firmware,

applications, middleware, metadata, and security attributes. Enterprise integrity verification tools include file integrity monitoring, endpoint detection and response, database integrity monitoring, and code signing enforcement.

b. Take appropriate actions when unauthorized changes are detected, including notifying the system owner, data owner, system administrator, and ETSS Security Operations personnel. Detected integrity violations shall generate alerts in the enterprise SIEM and trigger the incident response workflow. Affected systems may be isolated and restored from verified backups.

4.6.1 Integrity Checks (SI-7(1))

Applies to: Moderate and above (IAL2)

Each agency shall perform integrity checks of software, firmware, and information at system startup, at defined transitional states, on a continuous basis where technically feasible, after unplanned system shutdowns or process aborts, and immediately following the installation of new hardware, software, or firmware.

4.6.2 Integration of Detection and Response (SI-7(7))

Applies to: Moderate and above (IAL2)

Each agency shall incorporate the detection of unauthorized security-relevant changes to the information system into the agency incident response capability, including unauthorized changes to baseline configuration settings, unauthorized elevation of system privileges, and changes to or attempts to remove security agents on endpoints. See ETSS Incident Response Policy (300.x) for additional requirements.

4.7 Spam Protection (SI-8)

Applies to: Moderate and above (IAL2)

ETSS shall centrally manage spam protection mechanisms wherever possible. Each agency shall:

a. Employ spam protection mechanisms at information system entry and exit points to detect and act on unsolicited messages. Enterprise spam protection includes advanced threat protection capabilities such as attachment sandboxing and URL rewriting for phishing detection.

b. Update spam protection mechanisms when new releases are available in accordance with ETSS Configuration Management Policy (500.x).

4.7.1 Automatic Updates (SI-8(2))

Applies to: Moderate and above (IAL2)

Spam protection mechanisms shall be automatically updated when updates are available from tool vendors or upon receipt of threat intelligence or investigation findings. Automatic updates shall be enabled and monitored to ensure continuous protection without requiring manual intervention.

4.8 Information Input Validation (SI-10)

Applies to: Moderate and above (IAL2)

Information systems shall check the validity of information inputs (including syntax, format, length, parameters, and character set) for all system input fields and ingress points as defined in the applicable System Security Plan. Input validation shall prevent executable content from being unintentionally interpreted as commands, such as cross-site scripting and injection attacks.

4.9 Error Handling (SI-11)

Applies to: Moderate and above (IAL2)

Information systems shall:

a. Generate error messages that provide only the information necessary for

corrective actions and that do not reveal information which could be exploited by attackers.

b. Reveal error messages only to designated agency personnel, including system administrators, technical support personnel, and security personnel.

4.10 Information Management and Retention (SI-12)

Applies to: All systems (IAL1, IAL2)

Each agency shall handle and retain information within the information system and information output from the system for the full lifecycle of the information in accordance with applicable federal and State laws, Executive Orders, directives, and ETSS policies and standards. See Rhode Island Secretary of State Records Management and agency operational requirements, whichever is more restrictive. In the absence of any retention guidance, information shall be retained for a minimum of six (6) months.

4.11 Memory Protection (SI-16)

Applies to: Moderate and above (IAL2)

Each agency shall implement safeguards to protect memory from unauthorized code execution, including controls that prevent data execution (DEP) and randomize address space layout (ASLR). Systems administrators shall increase scrutiny of non-executable regions of memory and memory locations that are prohibited, which are commonly used to launch attacks with executable code.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Revocation or suspension of system access or administrative privileges.

b. Mandatory remediation of identified flaws within the timelines defined in this policy.

c. Formal counseling or written reprimand.

d. Referral to agency management for disciplinary proceedings.

e. Denial of system authorization for systems that do not meet flaw remediation or malicious code protection requirements.

f. Escalation to ETSS leadership for systemic non-compliance affecting enterprise security posture.

Failure to install security-relevant updates within established timelines, disabling or circumventing malicious code protection mechanisms, or tampering with system monitoring tools may be treated as security incidents and investigated accordingly. Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded in the agency Plan of Action and Milestones (POAM).

6. Roles and Responsibilities

The following roles are accountable for the implementation, monitoring, and enforcement of this policy:

Chief Information Security Officer (CISO)

Designated as the official responsible for the enterprise System and Information Integrity policy and procedures. Oversee the continuous monitoring program, flaw remediation benchmarks, security alert dissemination, and the integration of integrity detection with incident response capabilities.

ETSS Security Operations

Responsible for centrally managing malicious code protection, endpoint detection and response, SIEM operations, spam protection, and system monitoring across the enterprise. Receives and triages security alerts, investigates integrity violations, and executes incident response procedures.

ETSS Infrastructure and Operations (I&O)
Responsible for enterprise patch management, automated flaw remediation deployment, system backup and recovery for integrity restoration, and coordination of vulnerability scanning. Supports memory protection and configuration baseline enforcement across enterprise platforms.

System Owners
Responsible for ensuring flaw remediation is performed within established timelines for their systems, maintaining system-specific monitoring and integrity verification, coordinating with ETSS on malicious code protection for agency-managed systems, and ensuring information retention requirements are met.

Agency Information Managers (AIMs) / Technical Support Managers (TSMs)
Coordinate system and information integrity activities at the agency level, receive and disseminate security alerts and advisories, and ensure agency compliance with flaw remediation and malicious code protection requirements.

All Personnel
Responsible for reporting suspected malicious code, system anomalies, and security incidents to the ETSS Service Desk immediately. Must not disable or circumvent malicious code protection mechanisms or system monitoring controls.

7. Approval / Review Signatures


Digitally signed by Nathan Loura
Date: 2026.07.15 10:47:53 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.07.15 11:28:38 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services