Division of Enterprise Technology Strategy and Services

ETSS Policy 100.2

System Maintenance (MA)

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 the effective and secure maintenance, repair, and diagnostic servicing of State of Rhode Island information systems and system components. It defines requirements for controlled maintenance activities performed on-site or off-site, the management and inspection of maintenance tools, non-local (remote) maintenance, the authorization of maintenance personnel, and timely maintenance support. These requirements ensure the confidentiality, integrity, and availability of State data throughout all maintenance activities.
This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Maintenance family), 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.
This policy applies to all types of maintenance performed by any local or non-local entity (including in-contract, warranty, in-house, and software maintenance agreement) on any system component, including applications and components not directly associated with information processing or data retention (such as scanners, copiers, and printers).

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. Any new definitions introduced in this policy will be reviewed by the IT Governance and Policy Lead and incorporated into the Glossary as appropriate.

Controlled Maintenance
Scheduled, corrective, preventive, or emergency maintenance activities performed

Related Policies: Enterprise Policies

on information systems or system components that are planned, approved, documented, and reviewed in accordance with enterprise standards and manufacturer specifications.

Maintenance Tools
Hardware, software, or firmware used specifically for repairing, diagnosing, or servicing information systems and system components (such as packet sniffers, diagnostic test equipment, and firmware update utilities). For the purposes of this policy, maintenance tools do not include tools that are part of the standard operating environment of the information system (such as ping or ipconfig).

Non-local Maintenance
Maintenance and diagnostic activities performed by personnel communicating through an internal or external network connection (remote maintenance), rather than being physically present at the facility where the system resides.

Maintenance Personnel
Individuals that are authorized to perform maintenance, repair, or diagnostic activities on information systems or system components. Maintenance personnel may include ETSS staff, agency technical personnel, or approved vendor and contractor personnel.

4. Procedures for Compliance

The following requirements establish the system maintenance 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. Controls designated as applicable to all systems (IAL1 and IAL2) represent the minimum standard. Controls designated as IAL2 only apply to systems that store, process, transfer, or communicate classified data, including Personally Identifiable Information (PII), Federal Tax Information (FTI), or other sensitive data types.

4.1 System Maintenance Policy and Procedures (MA-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a system maintenance policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The policy shall address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance requirements. Maintenance procedures shall be integrated into ETSS operational workflows and system lifecycle management practices.

The ETSS Chief Technology Officer (CTO) is designated as the official responsible for the development, documentation, approval, and dissemination of the enterprise maintenance policy and procedures.

The agency shall review and update the system maintenance policy at least every three (3) years or following significant changes to technologies, regulatory requirements, or the threat environment. Supporting procedures shall be reviewed in alignment with the policy and updated following significant changes.

4.2 Controlled Maintenance (MA-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Schedule, perform, document, and review records of maintenance and repairs of

information systems or system components in accordance with manufacturer and vendor specifications and ETSS and agency requirements. All maintenance activities shall be tracked in ServiceNow in accordance with the change approval process and ETSS operational standards.

b. Monitor and approve all maintenance activities of information systems or system components, whether performed on-site or remotely. Remote maintenance shall be conducted using secure, authenticated administrative tools and approved access methods.

c. Require explicit approval from the system owner to remove any information system or system component from agency premises for off-site maintenance. Asset custody and chain-of-control requirements shall be enforced.

d. Sanitize equipment to remove classified data from associated media prior to removal from agency premises for off-site maintenance, in accordance with ETSS Media Protection and Data Classification policies.

e. Verify that all potentially impacted security controls are still functioning properly following maintenance or repairs, including verification of configuration baselines, security tooling (such as endpoint protection agents), and vulnerability posture.

f. Include within maintenance records the following information: date and time of the maintenance activity, name of the individual approving the maintenance, name of the individual or group performing the maintenance, name of the information system or system component (including any applicable State asset tag ID), purpose and description of the maintenance performed, and verification results.

4.3 Maintenance Tools (MA-3)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Approve, control, and monitor information system maintenance tools, techniques, and mechanisms used for diagnostic and repair actions on agency information systems or system components. Approved tools shall be restricted to authorized personnel and integrated with enterprise identity and access management controls. Maintenance tools shall be documented, approved by the system owner, and maintained in accordance with recommended vendor maintenance schedules. If a maintenance tool is maintained by a vendor, an appropriate contract or Service Level Agreement (SLA) shall be in place. Maintenance tools shall be disconnected from the information system or system component when maintenance activities have been completed. Use of maintenance tools shall be logged and auditable.

b. Review previously approved information system maintenance tools, techniques, and mechanisms at major technology, regulatory, or solution changes.

4.3.1 Inspect Tools (MA-3(1))

Applies to: Moderate and above (IAL2)

Each agency shall inspect maintenance tools carried into an agency facility for improper or unauthorized modifications prior to allowing the tool to be connected to the information system or system component.

4.3.2 Inspect Media (MA-3(2))

Applies to: Moderate and above (IAL2)

Each agency shall check media containing test and diagnostic programs for malicious code prior to the media being used in the information system.

4.3.3 Prevent Unauthorized Removal (MA-3(3))

Applies to: Moderate and above (IAL2)

Each agency shall prevent the removal of maintenance equipment containing State data or non-State information for which the agency serves as the information steward, by implementing one or more of the following methods:

a. Verify there is no State data maintained on the equipment.

b. Sanitize or physically destroy the equipment.

c. Retain the equipment within the facility, applying physical access controls and asset tracking mechanisms.

d. Obtain explicit written authorization from the system owner or designated Information Owner that authorizes the removal of the equipment from the facility. Approval shall be documented, time-bound, and stored within ServiceNow with the artifact of the change, including justification, scope, and risk acceptance details.

4.4 Non-local Maintenance (MA-4)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Explicitly approve and monitor non-local (remote) maintenance and diagnostic activities. Authorization shall be documented and tracked through ServiceNow, including scope, duration, personnel involved, and systems impacted. Non-agency personnel performing non-local maintenance shall be monitored in real time by agency personnel to ensure their actions are appropriate.

b. Allow the use of non-local maintenance and diagnostic tools only as consistent with ETSS and agency policy and procedures and as documented in the applicable System Security Plan. Established information system security controls shall not be bypassed to enable the performance of non-local maintenance and diagnostic activities.

c. Employ strong authentication controls, including multifactor authentication and enterprise identity management with role-based access, when establishing non-local maintenance and diagnostic sessions via external network connections. Sessions shall be established using encrypted communication channels that meet ETSS cryptographic standards. Privileged access for remote maintenance shall be granted on a least-privilege, time-bound basis and removed upon completion of maintenance activities.

d. Maintain records for nonlocal maintenance and diagnostic activities, including session activity, commands executed (where technically feasible), and connection metadata. Records shall be retained in accordance with ETSS audit and logging requirements.

e. Terminate sessions and network connections immediately upon completion of authorized non-local maintenance activities. Post-maintenance verification shall be performed to confirm system integrity, validate security control functionality, and ensure no unauthorized changes are introduced.

4.5 Maintenance Personnel (MA-5)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Establish a process for the authorization of maintenance personnel. Only authorized ETSS staff, approved agency technical personnel, or explicitly approved vendors shall be permitted to perform system maintenance and diagnostic activities. Authorization shall be role-based and aligned with job responsibilities, system ownership, and operational need.

b. Maintain a list of authorized maintenance personnel or contracted vendors.

c. Verify that non-escorted personnel performing maintenance on the information system possess the required access authorizations.
d. Designate organizational personnel with required access authorizations and technical competence to escort and supervise maintenance activities of personnel who do not possess the required access authorizations.

4.6 Timely Maintenance (MA-6)

Applies to: Moderate and above (IAL2)
Each agency shall obtain maintenance support and spare parts for critical information system and network components within a timeframe that supports advertised uptime, availability, Return to Operation (RTO), and Recovery Point Objective (RPO) requirements based on the criticality and risk of the specific asset or service. Maintenance support includes vendor support agreements, enterprise service contracts, and internal operational support models, prioritized based on system criticality, operational impact, and risk to the confidentiality, integrity, and availability of State information systems. Support shall be aligned with recovery objectives documented in agency IT contingency and business continuity requirements.

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 of maintenance access or system administration privileges.
b. Mandatory retraining on system maintenance requirements.
c. Formal counseling or written reprimand.
d. Referral to agency management and human resources for disciplinary proceedings, up to and including termination of employment.
e. Termination of vendor or contractor agreements for external maintenance personnel.
f. Referral to law enforcement if criminal activity is suspected.
Unauthorized maintenance activities, deliberate circumvention of maintenance controls, or failure to sanitize equipment prior to off-site removal 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 as findings 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 Technology Officer (CTO)
Designated as the official responsible for the enterprise System Maintenance policy and procedures. Oversee infrastructure and operations teams responsible for enterprise-level maintenance activities, vendor support agreements, and spare parts management.
Chief Information Security Officer (CISO)
Responsible for security review of maintenance activities, oversight of maintenance tool inspections, coordination with the Enterprise Security Team on maintenance-related security incidents and ensuring that security controls are verified following maintenance activities.
System Owners
Responsible for approving maintenance activities on their systems, authorizing off-site removal of equipment, maintaining lists of authorized maintenance personnel and vendors, and ensuring maintenance records are complete and accurate. System owners coordinate with

ETSS Infrastructure and Operations on scheduled and emergency maintenance.

ETSS Infrastructure and Operations (I&O)

Responsible for executing enterprise-level maintenance activities, managing vendor maintenance contracts, maintaining spare parts inventory for critical components, tracking maintenance activities in ServiceNow, and performing post-maintenance security control verification.

Technical Support Managers (TSMs) / Agency Information Managers (AIMs)

Responsible for coordinating maintenance activities at the agency level, ensuring agency compliance with this policy, escorting and supervising unauthorized maintenance personnel, and reporting maintenance-related security concerns to ETSS.

Maintenance Personnel (Internal and External)

Responsible for performing maintenance activities only within the scope of their authorization, following all applicable security procedures, disconnecting tools upon completion, and cooperating with inspection and monitoring requirements.

All Personnel

Responsible for reporting suspected unauthorized maintenance activities or tampering with information systems and system components.

7. Approval / Review Signatures

Sanjay Gupta

Digitally signed by Sanjay Gupta
Date: 2026.07.15 08:13:06 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2026.07.15 09:14:14 -04'00'

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