Division of Enterprise Technology Strategy and Services

ETSS Policy 500.1

Configuration Management Policy

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

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for managing the configuration of State of Rhode Island information systems and their components throughout the system development lifecycle. Effective configuration management reduces organizational risk by ensuring that changes to information systems are proposed, reviewed, approved, tested, and documented in a controlled manner, and that system baselines are maintained, monitored, and protected from unauthorized modification.
This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Configuration Management family), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements. Configuration management practices defined in this policy are aligned with the Information Technology Infrastructure Library (ITIL) Change Enablement framework adopted by ETSS and executed through the ServiceNow IT Service Management platform.

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 information systems, system components, and supporting infrastructure managed by or on behalf of ETSS and State agencies, including on-premises, cloud, and hybrid environments.

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.

Baseline Configuration
The documented set of technical, functional, and physical specifications that reflect the current

Related Policies: Enterprise Policies

approved state of an information system, including hardware, software, firmware, operating system and application versions, patch levels, configuration settings, and network topology.

Change Enablement

The ITIL practice for ensuring that changes to systems and services are assessed, authorized, and implemented in a controlled manner. ETSS implements Change Enablement through the ServiceNow Change Management module, with project-level tracking in JIRA.

Configuration Change Control

The systematic proposal, justification, implementation, testing, review, and disposition of changes to information systems, including modifications, upgrades, baseline changes, configuration setting changes, unscheduled changes, and vulnerability remediations.

Configuration Management

The process of establishing, maintaining, and managing changes to system hardware, software, documentation, and the functional and physical characteristics of the operational environment throughout the information system lifecycle.

Configuration Management Database (CMDB)

The centralized repository within ServiceNow serves as the authoritative source for tracking enterprise and agency system components, their attributes, ownership, relationships, and configuration status.

Configuration Settings

Parameters within information system hardware, software, or firmware components that can be changed and influence the security posture or functionality of the system.

Security Impact Analysis

An analysis of a proposed change to determine its potential impact on system security and privacy. Security impact analysis includes security plan reviews, risk assessments, and testing within a non-production environment.

4. Procedures for Compliance

The following requirements establish the configuration management 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 Configuration Management Policy and Procedures (CM-1)

Applies to: All systems (IAL1, IAL2)

The ETSS Tier 3 Platform / Service owner will document and disseminate a configuration management 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.

The Chief Technology Officer is responsible for baseline configuration standards and management at the enterprise level, including retention of previous configurations and oversight of infrastructure and operations teams that execute configuration changes. Delegates operational execution to ETSS platform owners, Infrastructure and Operations leadership, and agency IT leadership, and maintains oversight, and enforcement

authority.
f Portfolio and Project Management Office (CPMO) will ensure that review and updates to the configuration management policies occur at least every three (3) years or following significant changes to laws, regulations, technologies, or the threat environment. Supporting procedures shall be reviewed at least annually and following significant system or environmental changes.

4.2 Baseline Configuration (CM-2)
Applies to: All systems (IAL1, IAL2)
ETSS Tier 3 shall:

a. Develop, document, and maintain under configuration control a current baseline configuration of the information system that includes all system hardware, software, firmware, and documentation. Baselines shall include operating systems, applications, network devices, cloud services, and security tooling. The agency shall develop a diagram of the current system architecture that includes the network topology, configuration of peripherals, connections to other systems and networks, and the physical and logical placement of system components. Agencies should leverage Center for Internet Security (CIS) Benchmarks, IRS Office of Safeguards Computer Security Evaluation Matrix (SCSEM), or other approved benchmarks to ensure secure configurations. Where a configuration baseline benchmark does not exist for a system or resource, the vendor-recommended secure configuration or default factory settings shall be considered the baseline.

b. Review and update the baseline configuration at least annually, when directed by enterprise governance or authorizing officials, when system components are installed or upgraded, or when configuration settings change due to critical security patches, upgrades, or emergency changes. Configuration changes shall be tracked through formal change management processes using ServiceNow, with project-level tracking in JIRA, , and security attestation when needed within Archer, ensuring traceability and authorization.

4.2.1 Automation Support for Accuracy and Currency (CM-2(2))
Applies to: Moderate and above (IAL2)
Each agency shall employ automated mechanisms to maintain the accuracy, currency, completeness, and availability of the baseline configuration. These mechanisms include centralized configuration management platforms, endpoint management solutions, vulnerability scanning tools, and continuous monitoring systems. Automated tooling supports detection of unauthorized changes, configuration drift, and compliance deviations, enabling timely remediation and reporting.

4.2.2 Retention of Previous Configurations (CM-2(3))
Applies to: Moderate and above (IAL2)
Each agency shall retain the current version plus at least two (2) previous versions of baseline configurations (hardware, software, firmware, configuration files, and records) to support rollback, incident response, and system recovery activities. Configuration histories shall be maintained within enterprise configuration management systems, version-controlled repositories, and change management records. Daily system backups shall also be maintained in accordance with business continuity requirements.

4.2.3 Configure Systems, Components, or Devices for High-Risk Areas (CM-2(7))
Applies to: Moderate and above (IAL2)

Each agency shall:

Issue information systems, system components, or devices with pre-defined secure configurations (such as sanitized and encrypted storage, hardened configuration settings, and limited applications) to individuals traveling. All travel outside of the continental United States with State-issued devices must be approved and authorized through a ticketed service request that includes supervisor approval, justification, and destination. Locations designated as high risk (sanctioned, elevated cyber risk) are blocked via firewall configurations, and unauthorized travel results in automatic isolation of the ETSS asset via CrowdStrike until an approved release request is processed by the ETSS Security Operations team. Protection remains in enforcement until the user returns and the device is cleared.

4.3 Configuration Change Control (CM-3)

Applies to: Moderate and above (IAL2)

Change control shall be managed in accordance with the ITIL Change Enablement framework adopted by ETSS, executed through the ServiceNow Change Management module. Each agency shall:

a. Identify and document the types of changes to be placed under configuration control.

b. Review proposed changes to the information system and approve or deny such changes with explicit consideration for security and privacy impact analyses.

c. Document configuration change decisions (approvals and denials) associated with the information system.

d. Implement approved configuration-controlled changes to the information system.

e. Maintain a record of all implemented changes for the life of the information system.

f. Monitor and review activities associated with configuration changes to the information system.

g. Coordinate proposed changes with the ETSS Change Advisory Board (CAB) prior to implementing a change. System owners shall coordinate all normal and emergency (non-standard) configuration change activities with the CAB. Non-standard configuration change requests shall be initiated via the ServiceNow Service Management portal. Configuration change management shall be performed at a level commensurate with the size, complexity, and sensitivity of the information system, taking into consideration applicable Service Level Agreement (SLA) requirements. SLA contracts with external entities shall define the types of changes within the entity's environment that the agency must be informed of.

4.3.1 Testing, Validation, and Documentation of Changes (CM-3(2))

Applies to: Moderate and above (IAL2)

Each agency shall test, validate, and document changes prior to implementing information system changes in a production environment.

4.3.2 Security and Privacy Representatives (CM-3(4))

Applies to: Moderate and above (IAL2)

Each agency shall require the Agency Information Manager (AIM) and any other agency representatives with security and privacy-related knowledge and expertise to be informed of all configuration change control activities at the agency prior to implementing any ETSS CAB-approved change.

4.4 Impact Analysis (CM-4)

Applies to: All systems (IAL1, IAL2)

Each agency shall perform a security impact analysis of proposed changes to the information system to determine potential security and privacy impacts prior to implementation. Security impact analysis is a required element of the ETSS Change Management process. The analysis shall be performed by appropriate personnel (such as system administrators, agency security or privacy managers, or system engineers) and scaled in accordance with the security category of the information system.

4.4.1 Verification of Controls (CM-4(2))

Applies to: Moderate and above (IAL2)

Upon implementation of information system changes, each agency shall verify that impacted security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome regarding meeting the security and privacy requirements of the information system.

4.5 Access Restrictions for Change (CM-5)

Applies to: All systems (IAL1, IAL2)

Each agency shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. Only authorized and qualified individuals may access the information system or system components for the purpose of initiating a change. See ETSS Physical and Environmental Security Policy 10-16 (PE-3) and ETSS Access Control Policy 10-10 (AC-3) for additional requirements.

4.5.1 Automated Access Enforcement and Audit Records (CM-5(1))

Applies to: Moderate and above (IAL2)

Each agency shall employ automated mechanisms to enforce access restrictions for change and generate audit records of enforcement actions. Automated enforcement mechanisms shall support the detection of unauthorized or unapproved change attempts, ensure that change access is limited to authorized personnel, and produce auditable records of all change-related access events.

4.5.2 Privilege Limitation for Production and Operation (CM-5(5))

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Limit privileges to change system components and system-related information within a production or operational environment.

b. Review and reevaluate privileges at least quarterly to ensure they remain appropriate and aligned with current role assignments and operational needs.

4.6 Configuration Settings (CM-6)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Establish and document, within the baseline configuration, the most restrictive information system configuration settings consistent with operational requirements. Configuration baselines shall be aligned with the system's IAL categorization, the NIST 800-53 Moderate control baseline, CIS Level 1 Configuration Baseline, enterprise security policies and standards, vendor-recommended secure configurations, and applicable federal and state compliance requirements. Documented configuration benchmarks and security checklists are available from the National Institute of Standards and Technology (NIST) National Checklist Program and the Center for Internet Security (CIS).

b. Implement the approved configuration settings using centralized management and automation tools across enterprise-managed and agency-managed environments.

c. Document and approve deviations from established configuration settings for

individual system components within the System Security Plan, based on explicit operational requirements. Exceptions shall include justification, compensating controls, and expiration criteria, and shall be tracked through enterprise risk management and POAM processes.

d. Continuously monitor configuration settings to detect drift, unauthorized changes, or degradation of secure configurations. Findings shall be reviewed and remediated in coordination with system owners and technical teams.

4.7 Least Functionality (CM-7)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Configure the information system to provide only essential capabilities based on the principle of least privilege (see ETSS Access Control Policy 10-10, control AC-6).

b. Prohibit, restrict, or disable programs, functions, ports, protocols, and services that are not essential to the information system's mission and business functions. A list of essential programs, functions, ports, protocols, and services shall be documented in the applicable System Security Plan, including the definition of essential items, the use of nonessential items, and restrictions or prohibitions on nonessential items.

4.7.1 Periodic Review (CM-7(1))

Applies to: Moderate and above (IAL2)

Each agency shall review the information system at least quarterly to identify and disable unnecessary and nonsecure functions, ports, protocols, and services no longer required for agency mission and business functions.

4.7.2 Prevent Program Execution (CM-7(2))

Applies to: Moderate and above (IAL2)

The information system shall prevent the execution of software programs in accordance with ETSS and agency policies, rules of behavior, access agreements, and any terms and conditions regarding authorized use of software programs.

4.7.3 Authorized Software: Allow-by-Exception (CM-7(5))

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Identify software programs not authorized to execute on the information system.

b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.

c. Review and update the list of authorized software programs at least annually.

4.8 System Component Inventory (CM-8)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and maintain an inventory of information system components using the enterprise Configuration Management Database (CMDB) within the IT Service Management Platform (ServiceNow) as the authoritative source. The inventory shall:

a. Accurately reflects the current information system, including all system hardware, software, firmware, and documentation.

b. Include all components within the information system, including hardware specifications (manufacturer, model, serial number, physical location, system owner), software platforms and applications (software version and license information), and networked components (machine names, network addresses).

External information systems and system components used to process, store, or transmit State data, including contracted services (IaaS, PaaS, SaaS), shall be catalogued.

c. Not include duplicate accounting of system components or components assigned to any other information system.

d. Be at the level of granularity necessary for appropriate tracking and reporting, including all asset information required for ServiceNow catalog item record management.

The inventory shall be reviewed and updated at least quarterly or upon significant technology changes. Automated discovery mechanisms shall be used to populate and update inventory records from endpoint management, vulnerability scanning, cloud management, and network monitoring tools.

4.8.1 Updates During Installation and Removal (CM-8(1))

Applies to: Moderate and above (IAL2)

Each agency shall update the inventory of information system components as an integral part of component installations, removals, and information system updates.

4.8.2 Automated Unauthorized Component Detection (CM-8(3))

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Employ automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized hardware, software, or firmware components within the information system.

b. Upon detecting an unauthorized component, disable component network access, isolate the component if possible, and notify designated personnel.

4.9 Configuration Management Plan (CM-9)

Applies to: Moderate and above (IAL2)

Each agency shall develop, document, and implement a Configuration Management Plan (CMP) for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures.

b. Establishes a process for identifying and managing configuration items throughout the System Development Lifecycle (SDLC). See ETSS System and Services Acquisition Policy 10-17 for SDLC requirements.

c. Defines the configuration items to be placed under configuration management.

d. Is protected from unauthorized disclosure or modification.

e. Is reviewed at least annually and approved by designated personnel defined in the System Security Plan.

4.10 Software Usage Restrictions (CM-10)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Authorize and approve software prior to installation on agency endpoints and information systems, including governing the use of open-source software. Software shall adhere to secure configuration baseline checklists. All software implementations require formal approval through the ETSS Change Advisory Board (CAB).

b. Use and track software in accordance with licensing agreements, contract terms, and copyright and distribution laws. Detailed software asset management procedures, including subscription tracking, third-party software approval workflows, and freeware authorization processes, are documented in the ETSS

Software Asset Management Procedure and maintained separately from this policy.

c. Control and document the use of authorized peer-to-peer file sharing technology to ensure it is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Software with known vulnerabilities shall be mitigated in a timely manner through updates, patches, or hot fixes in accordance with the remediation timelines defined in ETSS Risk Assessment Policy 10-25 (RA-5). Software that has reached end-of-life (no longer supported or more than two revisions behind current) shall be identified for upgrade, and the agency shall develop and submit a plan to upgrade the software to the ETSS Enterprise Security Team for review.

4.11 User-Installed Software (CM-11)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Adhere to established ETSS policies and standards governing the installation of software.

b. Enforce software installation policies through documented methods, using automated methods where feasible. Non-privileged users shall not have local administrator privileges to install software and are required to obtain authorization and approval from the agency Technical Support Manager (TSM) for software installation. The agency shall contact ETSS Enterprise Security for authorization and approval prior to installing any software not listed on the authorized software list or currently authorized for installation on State assets.

c. Monitor information systems for compliance. End users shall not install unapproved software on any State asset without prior approval from ETSS Enterprise Security.

4.12 Information Location (CM-12)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Identify and document the location of classified and sensitive information, including Personally Identifiable Information (PII), and critical information system components on which the information is processed or stored.

b. Identify and document users who have access to the information system and system components where the information is processed or stored.

c. Document changes to the location of critical information system components where the information is processed or stored.

4.12.1 Automated Tools to Support Information Location (CM-12(1))

Applies to: Moderate and above (IAL2)

Each agency shall use automated tools to identify the location of classified and sensitive information, including PII, to ensure adequate controls are in place to protect the information and individual privacy.

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 change management access or system administration privileges.

b. Mandatory retraining of configuration management 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 provider personnel.

f. Referral to law enforcement if criminal activity is suspected.

Unauthorized changes to production systems, deliberate circumvention of change control processes, or failure to follow established baseline configuration requirements 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 Information Security Officer (CISO)

Responsible for security review of configuration changes, oversight of security impact analyses, and coordination with the Enterprise Security Team on configuration-related security incidents and vulnerability remediation.

Chief Technology Officer (CTO)

Responsible for baseline configuration standards and management at the enterprise level, including retention of previous configurations and oversight of infrastructure and operations teams that execute configuration changes. Delegates operational execution to ETSS platform owners, Infrastructure and Operations leadership, and agency IT leadership, and maintains oversight, and enforcement authority.

Chief of the Portfolio and Project Management Office (PPMO)

Designated as the official responsible for driving the creation of configuration management policy and procedures and executing governance in support of configuration management activities.

ETSS Change Advisory Board (CAB)

Reviews and approves or denies proposed configuration changes to enterprise systems. Coordinates normal and emergency (non-standard) change activities. Ensure changes are assessed for security, operational, and business impact prior to implementation.

System Owners

Responsible for maintaining baseline configurations, developing Configuration Management Plans, managing system component inventories in the ServiceNow CMDB, and ensuring that configuration changes to their systems follow established change management processes.

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

Responsible for coordinating configuration management activities at the agency level, approving agency-level changes prior to CAB submission, managing software installation requests, and ensuring agency compliance with this policy. TSMs are notified by ETSS Security of unapproved software identified during system and network scans.

ETSS Infrastructure and Operations (I&O)

Responsible for implementing approved configuration changes to enterprise infrastructure, maintaining the CMDB, executing automated discovery and monitoring, and supporting baseline configuration maintenance.

All Personnel

Responsible for complying with software installation restrictions, reporting unauthorized system changes, and refraining from modifying system configurations without proper authorization.

7. Approval / Review Signatures

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.07.15 08:15:26 -04'00'

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


Digitally signed by Nathan Loura
Date: 2026.07.15 10:50:18 -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 11:29:35 -04'00'

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