Enterprise Technology Strategy and Services Policy 10-14

Configuration Management (CM)  
Brian Tardiff, CISO

Last Revision: 8/28/2020  
doa.entsec@doit.ri.gov

1. Purpose

Establish policy for effectively managing risk associated with changes to and that have an impact on information system configurations. Managing the implementation of system changes to maintain system security and reducing overall organizational risk.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments\(^1\) (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Baseline Configuration
The technical, functional, and physical specifications that reflect the current information system architecture including, for example, standard software installed on workstations, laptops, servers, network components, and mobile devices, operating system and application versions and patch sets, and configuration settings.

Configuration Change Control
The systematic proposal, justification, implementation, testing, review, and disposition of changes to information systems, including system modifications and upgrades, changes to baseline configurations, changes to configuration settings, unscheduled changes, and changes to remediate vulnerabilities.

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

\(^1\) State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State colleges, the General Treasurer, the Attorney General, or the Secretary of State.
Configuration Management Plan
Defines system level processes and procedures for how configuration management will be implemented to support system development lifecycle activities and should describe how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how the development, test, and operational environments are controlled, and how documents are developed, released, and, updated.

Configuration Settings
Parameters within information system hardware, software, or firmware components that can be changed and, consequently, have an effect on 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. Security impact analysis tasks include security plan reviews, conducting risk assessments, and performing tests within a test environment.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Configuration Management Policy and Procedures (CM-1). The agency will develop, document, disseminate, review, and annually update a configuration management policy and procedures.

4.2. [IAL1, IAL2] Baseline Configuration (CM-2). The agency will develop, document, and maintain a baseline configuration of the information system. A diagram of the current system architecture will be developed that includes the network topology,
configuration of peripherals (e.g. printers, modems), connections to other IT system resources (e.g. shared printers, file servers) and networks, and physical and logical placement of system components within the system architecture.

4.2.1. \[IAL2\] Reviews and Updates (CM-2.1). The agency will review and update the baseline configuration of the information system on an annual basis and when required due to information system component installations and upgrades.

4.2.2. [IAL2] Retention of Previous Configurations (CM-2.3). The agency will retain the previous version (e.g. hardware, software, firmware, configuration files and records) of the baseline configuration for the information system to support rollback.

4.2.3. [IAL2] Configure Systems, Components, or Devices for High-Risk Areas (CM-2.7). The agency will issue devices that have pre-defined configurations (e.g. sanitized and encrypted storage drives, hardened configuration settings, limited applications) to individuals traveling to high-risk locations. Upon return from high-risk locations, the agency will apply security safeguards (e.g., examine to the devices for signs of tampering, re-imaging of storage drives).

4.3. [IAL1, IAL2] Configuration Change Control (CM-3). The agency will identify the types of changes to be placed under configuration control, review proposed changes to the information system, document configuration change decisions (approvals/denials) associated with the information system, maintain a record of all implemented changes for the life of the information system, and audit and review activities associated with configuration changes to the information system. The agency will review and coordinate proposed changes to information systems with the ETSS Change Approval Board (CAB) prior to implementing a change. Configuration management should be performed at a level commensurate with the size, complexity, and sensitivity of the information system, take into consideration Service Level Agreement (SLA) requirements, and be in accordance with documented ETSS policies. Resources (e.g. hardware, software, devices, data, personnel) necessary for proper configuration management should be documented and prioritized based on their classification, criticality, and business value to the agency. Automated mechanisms and controls should be deployed wherever possible to enhance security, facilitate the implementation of this policy, enforce access restrictions, centrally manage configuration settings, and maintain an up-to-date and readily available baseline system configuration.

4.3.1. [IAL2] Test, Validate, Document Changes (CM-3.2). The agency will test, validate, and document changes prior to implementing operating system changes.

4.4. [IAL1, IAL2] Security Impact Analysis (CM-4). The agency will perform an analysis of a proposed change to determine the potential impact to system security prior to the implementation of the proposed change. The security impact analysis should be performed by appropriate personnel (e.g. system administrator, agency security manager,
system engineer) and scaled in accordance with the security category of the information system.

4.5. [IAL1, IAL2] Access Restrictions for Change (CM-5). The agency will 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 its components for the purpose of initiating a change. See ETSS Physical and Environmental Security Policy 10-16 (section PE-3) and ETSS Access Control Policy 10-10 (section AC-3) for more information.

4.6. [IAL1, IAL2] Configuration Settings (CM-6). The agency will establish, document, and implement the most restrictive information system configuration settings consistent with operational requirements. Additionally, the agency will monitor and control changes to configuration settings in accordance with documented policies and procedures. Common secure configuration benchmarks (e.g. security checklists, hardening guides, and technical implementation guides) provide a standardized approach to implementing secure configuration settings to secure and meet operational requirements.

4.7. [IAL1, IAL2] Least Functionality (CM-7). The agency will configure the information system to provide only essential capabilities and prohibit or restrict the use of functions, ports, protocols, and services. Functions, ports, protocols, and services that are unused or not required for agency mission and business functions will be disabled.

4.7.1. [IAL2] Periodic Review (CM-7.1). The agency will review the information system annually to identify and disable unnecessary and nonsecure functions, ports, protocols, and services.

4.7.2. [IAL2] Prevent Program Execution (CM-7.2). The information system will prevent the execution of programs in accordance with ETSS and agency policies regarding software program usage and restrictions.

4.7.3. [IAL2] Unauthorized Software and Blacklisting (CM-7.4). The agency will (i) identify software programs not authorized to execute on the information system, (ii) employ an allow-all deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system, and (iii) review and update the list of unauthorized software programs annually.

4.8. [IAL1, IAL2] Information System Component Inventory (CM-8). The agency will document, maintain, and annually review and update, as required, an inventory of information system components that accurately reflects the current information system. The inventory will have a level of granularity that is necessary for appropriate tracking and reporting, should contain all necessary system component and software information, including hardware specifications (e.g. manufacturer, model, serial number, physical location, system owner), software platforms and applications (e.g. software version and license information), and networked components (e.g. machine names, network
addresses). External information systems and system components used to process, store, or transmit agency data, including contracted services (e.g. infrastructure/platform/software as a service), will be catalogued.

**4.8.1. [IAL2] Updates During Installations and Removals (CM-8.1).** The agency will update the inventory of information system components as an integral part of component installations, removals, and information system updates.

**4.8.2. [IAL2] Automated Unauthorized Component Detection (CM-8.3).** The agency will employ automated mechanisms, wherever possible, to detect the presence of unauthorized hardware, software, or firmware components within the information system and, upon detecting an unauthorized component, will disable component network access (e.g. disable ports, services), isolate the component (e.g. quarantine, sandbox), and/or notify designated personnel via an appropriate method (e.g. email, text).

**4.8.3. [IAL2] No Duplicate Accounting of Components (CM-8.5).** The agency will verify that components within the authorized boundary of the information system are not duplicated in other information system component inventories.

**4.9. [IAL1, IAL2] Configuration Management Plan (CM-9).** The agency will develop, document, protect from unauthorized disclosure or modification, and annually review and update, as required, a Configuration Management Plan (CMP) for the information system that (i) defines the roles, responsibilities, and configuration management processes and procedures, (ii) establishes a process necessary for identifying and managing configuration items throughout the System Development Lifecycle (SDLC), and (iii) defines the configuration items to be placed under configuration management. See ETSS System and Services Acquisition Policy 10-17 for more information regarding SDLC requirements.

**4.10. [IAL1, IAL2] Software Usage Restrictions (CM-10).** The agency will (i) authorize and approve software prior to it being installed on agency endpoints and information systems, (ii) use and track software in accordance with licensing, contract agreements, and copyright and distribution laws, and (iii) 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, and (iv) govern the use of open source software to ensure it is approved by the agency, legally licensed, and adheres to secure configuration baseline checklists (see https://www.nist.gov/programs-projects/security-configuration-checklists-commercial-it-products for more information).

**4.11. [IAL1, IAL2] User-Installed Software (CM-11).** The agency will (i) adhere to established ETSS policies and standards governing software approved for installation, (ii) enforce software installation policies through documented methods (if possible, via automated methods), and (iii) continuously monitor information systems for compliance. End users will not install software on any state asset without prior approval from ETSS.
5. Approval / Review Signature:

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2020.09.14 11:55:05 -04'00'

Chief Information Security Officer