# 140 – Configuration Management Standard

## Purpose

The Configuration Management Standard provides documentation of the minimum requirements for secure and compliant configuration of the Enterprise IT systems and system environments.

## Standard

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization.

Baseline secure and compliant IT system configurations must be based on one or more of the acceptable industry guidelines identified below. Exceptions, changes, or non-standard alterations to a secure and compliant configuration can be requested to meet a business or compliance need per the Enterprise Exception Procedure.

### Industry Guidelines

- Center for Internet Security (CIS) Benchmarks
- Defense Information Systems Agency (DISA) Standard Technical Implementation Guidelines (STIG)
- National Institute of Science and Technology (NIST) National Checklist Program
- United States Government Configuration Baselines (USGCB)
- National Security Agency Security Configuration Guides
- International Organization for Standardization (ISO)

### Primary Regulatory and Compliance Requirements (for Executive Branch Agencies)

- Centers for Medicare and Medicaid Services (CMS) - Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Criminal Justice Information Services (CJIS) Security Policy
- Family Educational Rights and Privacy Act (FERPA) Compliance

- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Social Security Administration (SSA) Technical System Security Requirements
- Wisconsin State Statutes Chapter 16.971

Agencies should consider the following for inclusion in their policies, procedures, or processes:

## Baseline Configuration (CM-2):

- Developing, documenting, and maintaining under configuration control, a current baseline configuration of the system; and
- Reviewing and updating the baseline configuration of the system:
  - Annually;
  - When required due to system changes; and
  - When system components are installed or upgraded.

### Automation Support for Accuracy and Currency (CM-2(2)):

- Maintaining the currency, completeness, accuracy, and availability of the baseline configuration of the system using Agency-defined automated mechanisms (i.e., configuration management tools, hardware, software, firmware inventory tools, or network management tools).

### Retention of Previous Configurations (CM-2(3)):

- Retaining previous versions of baseline configurations of the system to support rollback.

## Configuration Change Control (CM-3):

- Determining and documenting the types of changes to the system that are configuration-controlled;
- Reviewing proposed configuration-controlled changes to the system and approving or disapproving such changes with explicit consideration for security and privacy impact analyses;
- Documenting configuration change decisions associated with the system;
- Implementing approved configuration-controlled changes to the system;
- Retaining records of configuration-controlled changes to the system for the life of the system;
- Monitoring and reviewing activities associated with configuration-controlled changes to the system; and
- Coordinating and providing oversight for configuration change control activities through a change control board that convenes on a frequent basis (defined by the Agency).

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

- Testing, validating, and documenting changes to the system before finalizing the implementation of the changes.

### Security and Privacy Representatives (CM-3(4)):

- Requiring security and privacy representatives to be members of the change control board.

## Impact Analyses (CM-4):

- Analyzing changes to the system to determine potential security and privacy impacts prior to change implementation.

### Verification of Controls (CM-4(2)):

- After system changes, verifying that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

## Access Restrictions for Change (CM-5):

- Defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the system.

## Configuration Settings (CM-6):

- Establishing and documenting configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements;
- Implementing the configuration settings;
- Identifying, documenting, and approving the deviations from established configuration settings;
- Monitoring and controlling changes to the configuration settings in accordance with State and agency policies and procedures.

## Least Functionality (CM-7):

- Configuring the system to provide only the missions, functions, or operations deemed essential by the agency; and
- Prohibiting or restricting the use of functions, ports, protocols, software, and/or services to only those individuals/groups who require it for their job duties.

### Periodic Review (CM-7(1)):

- Reviewing the system annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
- Disabling or removing the functions, ports protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

### Prevent Program Execution (CM-7(2)):

- Preventing program execution in accordance with policies, rules of behavior, and/or access agreements regarding software program usage and restrictions as well as the rules authorizing the terms and conditions of software program usage.

### Authorized Software (CM-7(5)):

- Identifying the software programs authorized to execute on the system;
- Employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
- Reviewing and updating the list of authorized software programs annually.

## System Component Inventory (CM-8):

- Developing and documenting an inventory of system components that:
  - Accurately reflects the system;
  - Includes all components within the system;
  - Does not include duplicate accounting of components or components assigned to any other systems;
  - Is at the level of granularity deemed necessary for tracking and reporting; and
  - Includes the necessary information to achieve effective system component accountability.
- Reviewing and updating the system component inventory annually.

### Updates During Installation and Removal (CM-8(1)):

- Updating the inventory of the system components as part of component installations, removals, and system updates.

### Automated Unauthorized Component Detection (CM-8(3)):

- Detecting the presence of unauthorized hardware, software, and firmware components within the system using Agency-defined automated mechanisms on an ongoing basis; and
- Taking appropriate actions when unauthorized components are detected by disabling network access by such components, isolating the components, and/or notifying the appropriate personnel.

## Configuration Management Plan (CM-9):

- Developing, documenting, and implementing a configuration management plan for the system that:
  - Addresses roles, responsibilities, and configuration management processes and procedures;
  - Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
  - Defines the configuration items for the system and places the configuration items under configuration management;
  - Is reviewed and approved by Agency-defined appropriate personnel; and
  - Protects the configuration management plan from unauthorized disclosure and modification.

## Software Usage Restrictions (CM-10):

- Use software and associated documentation in accordance with contract agreements and copyright laws.
- Track the usage of software and associated documentation protected by quantity licenses to control copying and distribution.
- Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

## User-Installed Software (CM-11):

- If applicable, agencies develop policies and procedures for governing the installation of software by end users.
- Enforce software installation policies through Agency-defined methods.
- Agencies define a frequency on monitoring compliance.

### Information Location (CM-12):

- Identifying and documenting the location of agency information and the specific system components on which the information is processed and stored;
- Identifying and documenting the users who have access to the system and system components where the information is processed and stored; and
- Documenting changes to the location (i.e., system or system components) where the information is processed and stored.

## Additional Documentation:

- DET Change Management Policy
- DET Change Management Procedure
- DET Pre-Approved Change List
- DET Communication Listservs
- DET Weekly OPCOM Change Planning and Coordination (CPAC) Reports

## Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agencies.
State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to; network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by the Agency.
Identified Account Types include (AC-2): Individual, Privilege (Administrative and Default Privileged), Shared, Service, Emergency, and Temporary accounts.

## Exception Process

Exceptions to any Executive Branch Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies Exception Procedure.

## Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

| Version # | Revision or Review Date | Description of Change(s) | Reviewer/Author | Date Approved |
|---|---|---|---|---|
| 1.0 | 10/15/18 | Submitted to and approved by the IT Executive Steering Committee | Reviewer: ITESC<br>Author: DOA/DET | 10/15/18 |
| 1.0 | 10/29/19 | Reviewed with Agency Security Officers and feedback collected. Planning for making revisions. | Bureau of Security | 10/29/19 |
| 2.0 | 11/03/20 | Reviewed with Agency Security Officers and IT Directors and changes were incorporated | Reviewer: WI ISAC/ITDC<br>Author: DOA/DET/BOS | 11/11/20 |
| 3.0 | 06/24/22 | Reviewed with Agency Security Officers and IT Directors and changes were incorporated | Reviewer: ITESC<br>Author: DOA/DET | 06/24/22 |
| NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses. | | | | |

Authorized and Approved by:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227E849B429...

7/8/2022 | 1:55 PM CDT

Print/Type
Title

Signature

Date