Policy and Procedure 9-5
Information Security: Configuration Management

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	6/24/2024
Effective Date:	June 12, 2024		
Codes/Mandates:	Code of Virginia: §2.2-2007 and Code of Virginia, §2.2-2005		
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, ITRM Standard SEC530: Information Security Standard, ITRM Standard SEC502: Audit Security Standard		
Forms:	N/A		

CONTENTS

PURPOSE 1
SCOPE 1
DEFINITIONS and ACRONYMS 2
BACKGROUND 2
ROLES & RESPONSIBILITY 2
STATEMENT OF POLICY 3
Baseline Configuration (CM-2) 3
Configuration Change Control (CM-3) 4
Impact Analysis (CM-4) 5
Access Restrictions for Change (CM-5) 5
Configuration Settings (CM-6) 6
Least Functionality (CM-7) 6
System Component Inventory (CM-8) 7
Configuration Management Plan (CM-9) 8
Software Usage Restrictions (CM-10) 8
User-Installed Software (CM-11) 9
Information Location (CM-12) 9
Signed Components (CM-14) 9
AUTHORITY 9
INTERPRETATION 9
APPROVAL 9
Version History 9

PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that Department of Forestry develops, disseminates, and updates the Information Security: Configuration Management policy and procedure. This policy and procedure establishes the minimum requirements for the Information Security: Configuration Management.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.5 Configuration Management Family, Controls CM-1 through CM-14, as well as additional controls for the Commonwealth of Virginia.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all Department of Forestry information and information systems.

DEFINITIONS and ACRONYMS

"Agency" and **"DOF"** means the Virginia Department of Forestry.

"Data owner" means the agency manager or supervisor, designated by the state forester, who defines, manages and controls the use of data and ensures compliance with adopted standards.

"Information security officer" and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC530.

"System administrator" means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

"System owner" means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

ACRONYMS

CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DOF:	Department of Forestry
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
VITA:	Virginia Information Technology Agency

BACKGROUND

The Information Security: Configuration Management Policy and Procedure is intended to facilitate the effective implementation of the processes necessary to meet the Configuration Management requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy and procedure directs that the Department of Forestry meet these requirements for all IT systems.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

- Responsible (R) – Person working on activity
- Accountable (A) – Person with decision authority and one who delegates the work
- Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- Informed (I) – Person who needs to know of decision or action

Roles	Data Owner	System Owner	Information Security Officer
Tasks			
Develop, document, and maintain under configuration control, a current baseline configuration	R	A	R
Create and periodically review a list of agency hardware and software assets		R	A/R
Review and update the baseline configuration		R	A/R
Configuration change control	R	R	A/R
Security impact analysis	R	R	A/R
Define, document, approve, and enforce access restrictions		A	R
Limit information system privileges within a production environment		A	R
Establish, document, and implement configuration settings		A	R
Verify that the information system is configured for least functionality		R	A/R
Record and audit baseline security configurations		R	A/R
Preform and review it system vulnerability scans		R	A/R
Remediate system and application vulnerabilities		R	A/R
Information system component inventory		A	R
Configuration management plan		R	A/R

STATEMENT OF POLICY

In accordance with SEC530, CM-1 through CM-14 (Configuration Management), Department of Forestry will develop, disseminate, and update the Information Technology-Configuration Management Policy and Procedure on at least an annual basis. Department of Forestry shall control and document the configuration of information systems and their respective components.

Baseline Configuration (CM-2)

1. The ISO shall:

   a. Develop, document and maintain under configuration control, a current baseline configuration of the information system including communications and connectivity-related aspects of the system. At minimum, the baseline configuration shall include:

      i. Standard operating system/installed applications with current version numbers

      ii. Standard software load for workstations, servers, network components, and mobile devices and laptops

      iii. Up-to-date patch level information

      iv. Network topology

      v. Logical placement of the component within the system and enterprise architecture

      vi. Technology platform

   b. Maintain the baseline configuration of the information system to be consistent with the Department of Forestry's enterprise architecture.

c. Develop and maintain an organization-defined list of software programs authorized to execute on the information system.

d. Employ a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

e. Maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

f. Identify, document and apply more restrictive security configurations for sensitive agency IT systems, as necessary.

g. Maintain records that document the application of baseline security configurations.

h. Monitor systems for security baselines and policy compliance.

i. Reapply all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.

j. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

2. All COV users traveling outside of the United States of America (including territories and military bases) must utilize a loaner device in accordance with the organization-defined process; and Information Security Officers will verify the loaner devices that will be used for international travel meet the following controls:

   a. All operating system security updates, web browser software, Commonwealth Security and Risk Management security software and any necessary application software have been installed.

   b. Infrared ports, Bluetooth ports, web cameras and any hardware features, not needed for the trip, are disabled.

   c. If VPN is necessary, ensure it is installed and configured appropriately.

   d. All laptops and mobile telecommunication devices are encrypted, have sharing of all file and print services disabled and have ad-hoc wireless connections disabled

   e. All required cables and power adapters are packed with the devices.

3. The ISO shall create and periodically review of a list of agency hardware and software assets.

4. The ISO shall review and update the baseline configuration of the information system:

   a. Once a year at a minimum.

   b. When required due to a significant configuration change, such as an operating system upgrade or hardware change, or a demonstrated vulnerability.

   c. As an integral part of information system component installations and upgrades.

Configuration Change Control (CM-3)

The ISO or designee shall be responsible for the following:

1. Determine the types of changes to the information system that are configuration controlled.
2. Approve configuration-controlled changes to the system with explicit consideration for security impact analyses.
3. Document approved configuration-controlled changes to the system.
4. Retain and review records of configuration-controlled changes to the system.
5. Audit activities associated with configuration-controlled changes to the system;
6. Auditing of changes must include changes in activity before and after a change is made to the information system and the auditing activities required to implement the change.

7. Coordinate and provide oversight for configuration change control activities through an IT Security Team that convenes as needed to review changes prior to implementation.
8. Test, validate and document changes to the information system before implementing the changes on the operational system.
9. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures and the specific health, safety and environmental risks associated with a particular facility and/or process.
10. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible.
11. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.
12. Configuration change control for the information system shall involve the systematic proposal, justification, implementation, test/evaluation, review and disposition of changes to the system, including upgrades and modifications.
13. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls and routers), emergency changes, and changes to remediate flaws.
14. All changes to IT assets used by Department of Forestry shall be made in accordance with best practices as defined by the Information Technology Infrastructure Library (ITIL) framework.
15. Department of Forestry shall require that its service provider, document and implement configuration management and change control practices so that changes to the IT environment do not compromise security controls.

Impact Analysis (CM-4)

1. The ISO or designee shall analyze changes to the information system to determine potential security impacts prior to change implementation.
2. Individuals conducting security impact analyses must have the appropriate skills and technical expertise to analyze the changes to information system and the associated security ramifications.
3. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls.
4. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required.
5. Security impact analysis is scaled in accordance with the security categorization of the information system.
6. Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility or intentional malice.
7. After system changes, verify that the impacted controls are implemented correctly, operating as intended and producing the desired outcome regarding meeting the security and privacy requirements for the system.

Access Restrictions for Change (CM-5)

1. The system owner shall define, document, approve and enforce physical and logical access restrictions associated with changes to the information system.
   a. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

i. No local administrative rights will be granted without the submission of an exemption form and approval of the ISO.

b. Maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system.

i. Logical and physical access control lists that authorize qualified individuals to make changes to an information system or component must be created and maintained.

c. Access restrictions for change also include software libraries.

2. The system owner shall:

a. Limit information system developer/integrator privileges to change hardware, software and firmware components and system information directly within a production environment.

b. Review and reevaluate information system developer/integrator privileges quarterly and following an environmental change.

Configuration Settings (CM-6)

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters include, for example, registry settings; account, file and directory settings (i.e., permissions); and settings for services, ports, protocols and remote connections.

1. The system owner shall:

a. Establish and document mandatory configuration settings for information technology products employed within the information system using the Commonwealth of Virginia System Hardening Standards that reflect the most restrictive mode consistent with operational requirements.

i. A standard set of mandatory configuration settings must be established and documented for information technology products employed within the information system.

b. Implement the configuration settings.

c. Identify, document and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements.

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Least Functionality (CM-7)

The ISO or designee shall verify that the information system is configured to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols. and/or services that are not required for the business function of the information system.

1. Any exceptions to baseline security configurations must be documented by in writing and approved by the ISO or designee.
2. Department of Forestry shall require that the ISO maintains records confirming the implementation of baseline security configurations for each IT system.
3. Department of Forestry shall require that security baseline implementation records be audited annually by the ISO or designee, to verify the implementation of the appropriate baseline security configurations.
4. The ISO shall perform network vulnerability scans of all server and desktop computers on a frequency consistent with contractual service level agreements.
5. The ISO or designee shall review the results of the IT system vulnerability scans when completed.
6. Periodic review of systems will occur monthly and unnecessary and/or nonsecure functions, ports, protocols, software and services will be removed.

7. Department of Forestry shall require that sensitive internal-facing web applications are scanned for vulnerabilities on an annual basis. Sensitive external-facing web applications must be scanned for vulnerabilities monthly.

8. All identified operating system and application vulnerabilities will be remediated without undue delay according to the severity and risk according to CSRM guidelines.

9. Where feasible, the organization will limit component functionality to a single function per device (e.g., email server or web server, not both).

10. Code execution – binary or machine-executable code is only allowed in confined physical or virtual machine environments with the explicit approval of the ISO when such code is:

    a. Obtained from sources with limited or no warranty and/or

    b. Without the provision of source code.

11. Use or connection of unauthorized hardware is prohibited.

12. COV Technology Roadmaps will be used to identify hardware components for authorized use and the list of components will be reviewed and updated monthly.

System Component Inventory (CM-8)

1. The system owner shall develop, document and maintain an inventory of information system components that:

    a. Accurately reflects the system,

    b. Includes all components within the system,

    c. Does not include duplicate accounting of components or components assigned to any other system,

    d. Is at the level of granularity deemed necessary for tracking and reporting,

    e. Includes organization-defined information deemed necessary to achieve effective system component accountability,

    f. Includes assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

2. The system owner shall include in the system component inventory information, a means for identifying by name, position and role, individuals responsible and accountable for administering those components.

3. The system owner shall review and update the system component inventory on an annual basis and following an environmental change.

4. The system owner shall update the inventory of system components as part of component installations, removals and system updates.

5. The system owner shall maintain updated system and network diagrams.

6. The system owner shall include assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

7. The inventory of information system components must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:

    a. Manufacturer
    b. Type
    c. Model
    d. Serial number
    e. Physical location
    f. Software license information
    g. Information system/component owner
    h. Associated component configuration standard
    i. Software/firmware version information

j. Networked component/device machine name or network address
k. Ownership

Note: Data and homogeneous systems, belonging to Department of Forestry, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

Note: Where more than one agency may own the IT system and the agency or agencies cannot reach consensus on which should serve as system owner for the purposes of this Standard, upon request, the CIO of the Commonwealth will determine the system owner.

Configuration Management Plan (CM-9)

1. The ISO or designee shall develop, document and implement a configuration management plan for the information system that:

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

   b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.

   c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

   d. Assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

      i. In the absence of a dedicated configuration management team, the IT Director may be tasked with developing the configuration management process.

   e. Defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level.

   f. Describes 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 development, test and operational environments are controlledand finally, how documents are developed, released and updated.

2. The configuration management approval process must include:

   a. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system.

   b. Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

Software Usage Restrictions (CM-10)

1. The ISO or designee shall develop, document and implement a configuration management plan for the information system that:

   a. Use software and associated documentation in accordance with contract agreements and copyright laws.

   b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

   c. 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.

   d. Open-source software must be actively maintained by the software community, cannot contain proprietary code and must be distributed by a legitimate source.

2. USER-INSTALLED SOFTWARE

   a. User installed software is prohibited without the specific approval of the ISO or in the case of explicit privilege status, such as system administrator.

      i. Policy compliance will be monitored quarterly.

User-Installed Software (CM-11)

DOF prohibits user installed software unless approved by the ISO.

Information Location (CM-12)

1. The ISO or designee shall develop, document and implement a configuration management plan for the information system that:

   a. Identifies and documents the location of Commonwealth information and the specific system components on which the information is processed and stored.

   b. Identifies and documents the users who have access to the system and system components where the information is processed and stored.

   c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Signed Components (CM-14)

The ISO or designee will prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION

The director of information technology and chief of administration are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel
Director of Information Technology Name (Print)

DocuSigned by:
Parik Patel
3448F7C5358F457...
6/13/2024
Director of Information Technology Signature

Amanda Davis
Chief of Administration Name (Print)

DocuSigned by:
amanda davis
C2CCAB60F85A4A6...
6/13/2024
Chief of Administration Signature

Version History

Version History			
Date	**Version**	**Details**	**Author/Contributors**
June 12, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO