### IT Configuration Management Policy TEMPLATE

### 

**EFFECTIVE DATE: 07/01/2014**

**Configuration Management Policy Template**

# 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 “YOUR AGENCY NAME” develops, disseminates, and updates the IT Configuration Management Policy. This policy and procedure establishes the minimum requirements for the IT Configuration Management Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.5 Configuration Management Family, Controls CM-1 through CM-9, as well as additional controls for the Commonwealth of Virginia.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems

# ACRONYMS

CI: Configuration Item

CIO: Chief Information Officer

CIS: Center for Information Security

ISO: Information Security Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

IT: Information Technology

ITIL: Information Technology Infrastructure Library

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT Configuration Management Policy at “YOUR AGENCY NAME” 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 SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

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

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

# STATEMENT OF POLICY

In accordance with SEC501, CM-1 through CM-9 (Configuration Management), “YOUR AGENCY NAME” will develop, disseminate, and update the Configuration Management Policy on at least an annual basis. “YOUR AGENCY NAME” shall control and document the configuration of information systems and their respective components.

**A. BASELINE CONFIGURATION**

1. The ISO shall:
   1. 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:
      1. Standard operating system/installed applications with current version numbers,
      2. Standard software load for workstations, servers, network components, and mobile devices and laptops,
      3. Up-to-date patch level information,
      4. Network topology,
      5. Logical placement of the component within the system and enterprise architecture, and
      6. Technology platform.
   2. Maintain the baseline configuration of the information system to be consistent with the “YOUR AGENCY NAME”’s enterprise architecture.
   3. Develop and maintain an organization-defined list of software programs authorized to execute on the information system.
   4. Employ a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.
   5. Maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.
   6. Identify, document, and apply more restrictive security configurations for sensitive agency IT systems, as necessary.
   7. Maintain records that document the application of baseline security configurations.
   8. Monitor systems for security baselines and policy compliance.
   9. Reapply all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
   10. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.
2. The ISO shall create and periodically review of a list of agency hardware and software assets.
3. The ISO shall review and update the baseline configuration of the information system:
   1. Once a year at a minimum;
   2. When required due to a significant configuration change, such as an operating system upgrade or hardware change, or a demonstrated vulnerability; and
   3. As an integral part of information system component installations and upgrades.
4. **CONFIGURATION CHANGE CONTROL**
5. 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 a Change Control Board that convenes on a weekly basis 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 “YOUR AGENCY NAME” shall be made in accordance with best practices as defined by the Information Technology Infrastructure Library (ITIL) framework;
   15. Service provider shall make all changes to IT assets that it supplies for use by “YOUR AGENCY NAME” in accordance with ITIL best practices;
   16. An information security representative shall be a member of the configuration change control board; and
   17. “YOUR AGENCY NAME” 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.
6. **SECURITY IMPACT ANALYSIS**
7. The ISO or designee shall analyze changes to the information system to determine potential security impacts prior to change implementation.
   1. 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.
   2. 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.
   3. 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.
   4. Security impact analysis is scaled in accordance with the security categorization of the information system.
8. **ACCESS RESTRICTIONS FOR CHANGE**
9. The System Owner shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
   1. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.
      1. No local administrative rights will be granted without the submission of an exemption form and approval of “YOUR AGENCY NAME” Commonwealth Security and Risk Management (CSRM).
   2. 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.
      1. Logical and physical access control lists that authorize qualified individuals to make changes to an information system or component must be created and maintained.
   3. Access restrictions for change also include software libraries.
10. The System Owner shall:
    1. Limit information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and
    2. Review and reevaluate information system developer/integrator privileges annually.
11. **CONFIGURATION SETTINGS**

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:
   1. 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;
      1. A standard set of mandatory configuration settings must be established and documented for information technology products employed within the information system.
   2. Implement the configuration settings;
   3. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
   4. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
2. **LEAST FUNCTIONALITY**
3. 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. “YOUR AGENCY NAME” has developed system hardening baselines for the operating systems known to be in use within the agency. “YOUR AGENCY NAME” will also utilize the system hardening baselines established by The Center for Internet Security (CIS) for those systems not addressed by the “YOUR AGENCY NAME”-specific system hardening baselines.
   2. In cases where a baseline security configuration does not exist for an operating system, the ISO or designee shall ensure a baseline security configuration is developed, documented and approved.
   3. Security operations staff shall apply these baseline security configurations to all operating systems. Where “YOUR AGENCY NAME”/CIS documents level 1 and level 2 baseline security configurations, unless otherwise approved by the ISO, “YOUR AGENCY NAME” shall use:
      1. Level 1 configurations for internal IT systems; and
      2. Level 2 configurations for internet- and/or customer-facing IT systems.
   4. Any exceptions to baseline security configurations must be documented by security operations staff in writing and approved by the ISO or designee.
   5. “YOUR AGENCY NAME” shall require that security operations staff maintain records confirming the implementation of baseline security configurations for each IT system they manage.
   6. “YOUR AGENCY NAME” 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.
   7. “YOUR AGENCY NAME” shall require that security operations staff perform network vulnerability scans of all server and desktop computers on a frequency consistent with contractual service level agreements.
   8. The ISO or designee shall review the results of the IT system vulnerability scans when completed.
   9. “YOUR AGENCY NAME” 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 on a quarterly basis. This scanning may be performed by security operations staff, system owners or Commonwealth Security and Risk Management staff as is appropriate and convenient.
   10. All identified operating system and application vulnerabilities will be remediated without undue delay according to the severity and risk utilizing the “YOUR AGENCY NAME”’s Change Management Policy and Procedure.
   11. Where feasible, the organization will limit component functionality to a single function per device (e.g., email server or web server, not both).
4. **INFORMATION SYSTEM COMPONENT INVENTORY**
5. The System Owner shall develop, document, and maintain an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Is consistent with the authorization boundary of the information system;
      1. All components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.
   3. Is at the level of granularity deemed necessary for tracking and reporting;
   4. Includes organization-defined information deemed necessary to achieve effective property accountability, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address;
      1. Updated system and network diagrams must be maintained.
   5. Is available for review and audit by designated organizational officials;
   6. Is updated as an integral part of component installations, removals, and information system updates;
   7. Is included in property accountability information, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components; and
      1. A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.
   8. Includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.
6. 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:
   1. Manufacturer,
   2. Type,
   3. Model,
   4. Serial number,
   5. Physical location,
   6. Software license information,
   7. Information system/component owner,
   8. Associated component configuration standard,
   9. Software/firmware version information, and
   10. Networked component/device machine name or network address.
   11. Ownership

Note: Data and homogeneous systems, belonging to “YOUR AGENCY NAME”, 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.

1. **CONFIGURATION MANAGEMENT PLAN**
2. The ISO or designee shall develop, document, and implement a configuration management plan for the information system that:
   1. Addresses roles, responsibilities, and configuration management processes and procedures;
   2. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management;
   3. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items;
   4. Assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development;
      1. In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process.
   5. Defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level; and
   6. 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 controlled, and finally, how documents are developed, released, and updated.
3. The configuration management approval process must include:
   1. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system, and
   2. Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 09/28/2007 | Original |
| 2 | 06/25/2010 | Updated to be in compliance with the ITRM Information Security Standard – SEC501 (Revision 5) dated 08/11/2009. |
| 2.1 | 08/06/2010 | Updated link for COV Information Security Policy, ITRM (SEC519-00). |
| 3 | 02/01/2013 | Administrative changes |
| 4 | 07/01/2014 | Complete rewrite of the “YOUR AGENCY NAME” CSRM IT System Security Configuration Policy in compliance with the ITRM Information Security Standard SEC501 Revision 8 with Role Matrix added. |
| 5 | 11/12/2021 | Formatting changes |