Commonwealth of Massachusetts

Executive Office of Technology Services and Security

Enterprise Risk Management Office

Enterprise Change and Configuration Management Policy

Document Name: Change and Configuration Management Policy	Effective Date: 1/1/2025
Document ID: ISP.006	Last Revised Date: 4/3/2025

Table of Contents

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum security requirements and key ***information*** security considerations that Commonwealth Agencies and Offices must implement as part of the following programs:

1.1.1. Operations Management

1.1.2. Change and Configuration Management

1.1.3. Release Management

1.1.4. Data Backup and Restoration

1.1.5. Cloud Computing

1.2. This ***policy*** reinforces the Commonwealth's commitment to an effective change and configuration management program and outlines the ***controls*** necessary to safeguard the Commonwealth's ***information assets*** and reduce ***risks*** posed by improper change and configuration management practices.

2. Authority

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security (EOTSS), possess the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. Scope

3.1. This document applies to the use of ***information***, ***information systems***, ***assets***, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, ***agencies***, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security (EOTSS), by any form of contractual arrangement, are required to comply with this document as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. Responsibilities

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***policy***. The Enterprise Risk Management Office is responsible for this ***policy*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***policy***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***policy*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. Additional ***information*** regarding this ***policy*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/policies.

4.3. In the event of any conflict between the provisions contained in this ***policy*** and the provisions set forth in any of the Enterprise Information Security Standards, the provisions in the Enterprise Information Security Policies will govern.

4.4. Definitions of terms in bold may be found in the *IS.Glossary of Terms* at https://www.mass.gov/cybersecurity/policies.

5. Compliance

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance.

5.3.2. Identify and explain in detail the ***risks*** created due to the non-compliance.

5.3.3. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level.

5.3.4. Specify the time-frame required to implement the ***controls*** and mitigate the identified ***risks***. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact ***information*** for both the ***risk owner*** and the ***control owner*** designated by the agency to accept and manage the ***risks*** associated with the non-compliance and implement the ***controls*** that will effectively mitigate the identified ***risks.***

6. Operations Management

6.1. Commonwealth Agencies and Offices must create, maintain, and update standard operating ***procedures*** to ensure the security of their critical and high-***risk information systems***. The standard operating ***procedures*** should, at a minimum, include the following:

6.1.1. Secure installation and configuration of systems.

6.1.2. Secure processing and handling of ***information*** (automated and manual).

6.1.3. System restart and recovery ***procedures*** to restore service in a timely manner in the event of system failure.

6.1.4. Logging requirements, including maintaining an audit trail for operational and security ***events***.

6.1.5. Support and escalation ***procedures***, including contact ***information*** of technical support staff.

7. Change Management

7.1. Commonwealth Agencies and Offices must implement a change management ***process*** that includes:

7.1.1. Definition of change request categories (High, Medium, Low ***risk***).

7.1.2. Definition of the change request approval ***process***, including the level of involvement of the Change Advisory Board — High and Medium ***risk*** must be approved by the Change Advisory Board.

7.1.3. Identification and documentation of all change requests in a system of record to maintain an audit trail.

7.1.4. Planning and testing of changes prior to implementation.

7.1.5. Verification that ***information*** security and regulatory compliance requirements have been met.

7.1.6. Definition of the emergency change request ***process***. Emergency change requests should be regularly audited to ensure the ***process*** is being used for its intended purpose.

8. Configuration Management

8.1. Commonwealth Agencies and Offices must establish ***controls*** to maintain the integrity of ***information systems***, including:

8.1.1. Maintain an ***asset*** inventory of authorized hardware and ***software***.

8.1.2. Update the ***asset*** inventory on a regular basis, but not less than annually.

8.1.3. Deploy network tools to detect and monitor the presence of hardware and ***software*** operating within the environment.

8.1.4. Establish an action plan to address unauthorized or unsupported ***information systems*** on the network.

8.1.5. Assess compliance with configuration requirements at least annually.

8.1.6. Establish security hardening guidelines for ***information systems***.

8.1.7. Assess compliance with security hardening requirements at least annually.

8.1.8. Obtain ***Secretariat CISO*** approval prior to implementing changes to network devices. Changes must be implemented by qualified ***personnel***.

8.1.9. ***Log*** configuration changes to ***information systems*** and ***applications***.

9. Capacity Management

9.1. Commonwealth Agencies and Offices must establish a capacity management plan for mission critical systems that includes the following:

9.1.1. Perform periodic server consolidation assessments to reduce the IT footprint.

9.1.2. Decommission ***applications***, databases and systems that are not required within an acceptable timeframe.

9.1.3. ***Information systems*** that must remain operational beyond their end-of- life (e.g., vendor support life cycle) will require a policy non-compliance report to be filed as detailed above.

9.1.4. Commonwealth Agencies and Offices are responsible to monitor and plan for hardware and ***software*** as they approach obsolescence.

10. Release Management

10.1. Commonwealth Agencies and Offices must document release management ***processes*** for IT environments and/or platforms that include the following:

10.1.1. Maintain separate development, test, and production environments.

10.1.2. Source code must be reviewed and tested in a lower environment prior to promotion to the production environment.

10.1.3. Production ***data*** may only be used in a test, or non-production environment after a policy non-compliance report is filed as detailed above.

10.1.4. The security ***controls*** for the test, or non-production environment are consistent with the production environment.

10.1.5. Developers must not have the ability to migrate code into production environments.

10.1.6. If a dedicated release management role is not in place, Commonwealth Agencies and Offices must ensure that ***personnel*** are issued separate accounts to perform their release management duties.

11. Data Backup and Restoration

11.1. Commonwealth Agencies and Offices must establish a ***process*** to back up ***information*** in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

11.1.1. Backup and recovery must be included as part of business continuity and disaster recovery planning.

11.1.2. Backup records subject to legal holds will be managed in accordance with guidance provided by EOTSS' Legal.

11.1.3. Backup ***data*** should be retained and written to long-term secure storage to comply with all applicable record retention requirements.

12. Cloud Computing

12.1. Commonwealth Agencies and Offices must establish ***procedures*** to ensure the secure implementation of ***applications*** and services in public and private cloud environments. Operational ***policies*** for cloud-based ***applications*** will, at a minimum, include the following:

12.1.1. Commonwealth Agencies and Offices will assign an ***application administrator*** for each ***application*** hosted in the cloud.

12.1.2. Service level agreements, including system uptime, availability, and scalability (bandwidth, storage, and transactional volume) metrics must be defined during the contracting phase and codified in contractual agreements.

12.1.3. Access to cloud-based ***applications*** must be role-based. Roles must be defined and documented.

12.1.4. ***Users*** with administrative privileges must have separate ***user*** accounts for normal activities. Use of administrative accounts must be logged and periodically audited.

12.1.5. Cloud-based ***application*** providers of critical-***risk*** or high-***risk*** systems must provide evidence of ***information*** security training and background checks for qualified ***personnel*** working on critical-***risk*** or high-***risk*** cloud ***applications*** for the Commonwealth.

12.1.6. ***Incident*** response plans, escalation ***procedures***, business continuity and disaster recovery plans for cloud-based systems must be documented for ***applications*** hosted in the cloud.

12.1.7. Cloud-based ***application*** providers will document their ***patch management process***. Critical security ***patches*** must be deployed as soon as technically feasible.

12.1.8. Cloud providers will notify Commonwealth Agencies and Offices in advance of any maintenance activities, specifically, for any update, upgrade or maintenance of ***software*** or hardware equipment that may impact system performance.

12.1.9. Cloud providers must implement security monitoring ***controls***, that will monitor and detect anomalous activity, detect and prevent intrusion and possess forensic capabilities to assist in an investigation, in the event of a security ***incident***, or breach.

12.1.10. Cloud providers will provide a mechanism to track performance metrics against contractual obligations, including ***information*** on major outages and time for resolution.

12.1.11. ***Data*** retention and retrieval periods, including the length of time within which the Commonwealth can retrieve its ***data*** from the cloud provider post contract termination must be clearly set forth in all cloud provider contracts.

12.1.12. Commonwealth Agencies and Offices will develop a contingency plan in the event a cloud service provider is acquired or goes out of business.

13. Roles and Responsibilities

Role	Responsibility
Commonwealth Chief Information Security Officer (CISO)/Chief Risk Officer (CRO)	The person responsible for ensuring compliance with this policy across all Commonwealth Agencies and Offices. The CISO leads the ERM Office and is responsible for aligning security initiatives with enterprise programs and business objectives. The CISO ensures that all of the Commonwealth's IT assets, communication systems, data and technologies are securely protected.
Enterprise Risk Management Office (ERM)	The office within EOTSS responsible for risk strategy, identification, assessment, analysis, monitoring, reporting and mitigation. Under the direction of the Commonwealth CISO/CRO, ERM establishes the Commonwealth's information security policies, standards, guidelines and directives to create an effective risk governance program that determines acceptable levels of risk tolerance and implements cybersecurity best practices to mitigate operational, reputational, security and financial risk.
Application Administrators	The person(s) within the Commonwealth Agency or Office responsible for managing cloud-based applications and the relationship with the cloud service providers.
Change Advisory Board (CAB)	Responsible for overseeing the change request process and ensuring all changes are reviewed for compliance and privacy considerations prior to implementation.

Commonwealth Agencies and Offices	Commonwealth Agencies and Offices are responsible to adhere to this policy and to comply with the requirements in this document in addition to any supporting documentation issued by the Secretary of EOTSS/Commonwealth CIO, the Commonwealth CISO/CRO, and/or the ERM office.

14. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Roles and Responsibilities	CM-03, CM-04, CM-09	-	GV.RR
Change Management	CM-03,	-	PR.PS-02, PR.PS-03, PR.PS-04
Configuration Management	CM-02, CM-03	4.1, 4.2, 4.3, 4.6, 12.2,12.3	PR.PS-01, PR.PS-04,

15. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/6/2024	Initial Policy Draft.
1.1	Thomas E. McDermott	7/9/2024	Revisions, Corrections, Formatting
1.2	Miklos Lavicska	8/9/2024	Correction, Formatting
1.3	Thomas E. McDermott	12/23/2024	Revisions, Corrections, Formatting
1.4	Anthony J. O’Neill	1/1/2025	Final Review
1.5	Thomas E. McDermott	4/3/2025	Updates, Corrections, Formatting
1.5	Miklos Lavicska	4/10/2025	Corrections and Formatting
1.5	Anthony J. O’Neill	4/18/2025	Final Review