Commonwealth of Massachusetts

Executive Office of Technology Services and Security
Enterprise Risk Management Office

Enterprise Software and Application Management Policy

Document Name: Software and Application Management Policy	Effective Date: 1/1/2025
Document ID: ISP.008	Last Revised Date: 4/4/2025

Table of Contents

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum security requirements that must be implemented to develop, test, install, manage, and terminate ***software*** programs, systems and ***applications***. This ***policy*** reinforces the Commonwealth's commitment to an effective ***software*** and ***application*** management program. This document outlines the ***controls*** that must be developed and incorporated into the ***software*** and ***application*** lifecycle, in order to safeguard ***assets*** and reduce ***risks*** posed by improper management of ***software*** and ***applications*** within the Commonwealth's ***information*** technology environment.

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 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. Requirements for Software and Application Management

6.1. Software and Applications

6.1.1. This ***policy*** applies to the use of any and all ***software*** and/or ***applications***, including ***software*** and/or ***applications*** purchased from ***third-party*** vendors, internally created, or otherwise acquired, any and all legacy ***software***, ***applications***, ***information systems***, electronic and computing devices, and network resources used to conduct business on behalf of the Commonwealth, hereinafter referred to as ***applications***.

6.1.2. Only currently supported and approved ***software*** and/or ***applications*** are authorized for use on any Commonwealth system or network.

6.1.3. Commonwealth Agencies and Offices must submit a policy non-compliance report as detailed above, in order to use any type of unsupported ***software*** and/or ***applications*** that have reached their end-of-life and/or are no longer supported by the developer/vendor, and/or ***software*** and/or ***applications*** for which the developer/vendor no longer provides updates, ***patches*** or new features.

6.1.4. Commonwealth Agencies and Offices will implement security ***controls***, to protect ***applications*** against malicious ***software***, such as viruses and ***malware,*** including those that may be introduced via removable media.

6.1.5. Commonwealth Agencies and Offices will Configure antivirus solutions so that they cannot be circumvented, disabled, or removed by an end ***user***, and implement technical ***controls*** to restrict the installation of unauthorized ***software*** on Commonwealth-owned or managed ***assets***.

6.2. Software and Application Ownership

6.2.1. Commonwealth Agencies and Offices will designate an ***information owner*** or an ***application administrator*** for all ***software*** and/or ***applications***. The designated owner will remain responsible for the management and security of the ***application,*** including ***application*** access, restrictions, and ***risk*** mitigation.

6.3. Software and Application Testing

6.3.1. All new ***applications*** must be thoroughly inspected, scanned, tested, and approved for use prior to their implementation. Records demonstrating the completion of such inspection, scanning, testing and approval will be maintained by the agency.

6.3.2. After their initial implementation, ***applications*** will be inspected, scanned, tested, and updated on a regular basis in compliance with EOTSS' Vulnerability Management Program, (VMP). Records demonstrating the completion of such subsequent inspection, scanning, testing and approval will be maintained by both EOTSS and the agency.

6.3.3. Commonwealth Agencies and Offices will inform EOTSS' VMP Manager of any ***application*** that is subsequently found to require removal, reinstallation, termination of use, or any other material change, other than a routine upgrade, or security ***patch***.

6.3.4. All ***third-party*** vendors who sell or otherwise provide any form of ***software*** to the Commonwealth are required to comply with both the EOTSS Vendor Risk Management Program and the Vulnerability Management Program.

6.3.5. The ***information owner*** or ***application administrator*** will ensure that all ***applications*** are tested prior to implementation and use, and on a regular basis throughout their lifecycle. ***Software*** and/or ***application*** testing will include, but may not be limited to penetration testing, ***vulnerability*** scanning, network monitoring, and static and dynamic code testing.

6.4. Software and Application Inventories:

6.4.1. All Commonwealth Agencies and Offices will identify, establish and maintain an inventory of all ***software*** and/or ***applications***.

6.4.2. Inventories must include all ***information*** necessary to effectively manage the ***application*** throughout its lifecycle, from creation through end of lifecycle disposal.

6.4.3. Inventories must be reviewed and updated on a continuous basis, but not less than quarterly.

6.4.4. Agencies will retain inventory reports in accordance with the statewide records retention schedule and provide copies of their inventory reports to EOTSS not less than quarterly.

6.5. Software and Application Risk Assessments

6.5.1. As part of the ***software*** and/or ***application*** design and development phase, Commonwealth Agencies and Offices will perform a high-level ***risk*** assessment. The initial ***risk*** assessment will identify any security-related requirements that must be implemented to mitigate any major concerns.

6.5.2. The development phase ***risk*** assessment will also determine whether or not the proposed ***software*** and/or ***application*** can operate within the agency's ***risk*** profile and should identify the initial set of key ***controls*** that must be incorporated into the design of the proposed ***software*** and/or ***application***.

6.5.3. The ***information owner*** or ***application administrator*** will be responsible to perform the high-level ***risk*** assessment.

6.5.4. Commonwealth Agencies and Offices will perform a high-level ***risk*** assessment for all significant changes to the ***application*** that involve security and/or privacy, (e.g., new ***software applications***, new ***software*** features, introduction of new systems and/or a significant modification to existing ***software application*** features or existing architecture).

6.5.5. ***Information*** and ***application owners*** will ensure that new or significantly changed systems and ***software applications*** are released to the production environment only after a pre-implementation security ***risk*** assessment and ***information*** security issues are addressed.

6.6. Separation of Environments and Protection of Data

6.6.1. Development, test, and production environments will be separated to reduce the ***risks*** of unauthorized access or changes to production systems and code repositories. Development, test, and production ***software*** will run on different systems or computer processors.

6.6.2. ***Access controls*** must be used to enforce access to the development, test, and production environments. Test environments must emulate the operating system environment as closely as possible.

6.6.3. ***Commonwealth Agencies and Offices*** will ensure that ***confidential*** production ***data*** is not copied into the test environment. The use of ***confidential*** production ***data*** in a non-production environment is prohibited, unless it is explicitly approved by the Commonwealth CISO, or his or her designee.

6.6.4. ***Confidential*** production ***data*** will be removed from test systems when it is no longer required. Test ***data*** must be removed from systems prior to going live in the production environment. Commonwealth Agencies and Offices will inform EOTSS when they remove the test data and when they are scheduled to go live in the production environment.

6.6.5. The ***Information Owner*** is responsible for ensuring that system inputs, outputs and processing functions are validated prior to production release in coordination with the development team.

6.7. Release Management Process

6.7.1. Releasing new systems and ***application software*** to the production environment must follow a defined ***process*** that ensures the integrity and accountability of all of the components released.

6.7.2. Systems and ***applications*** will not be released to the production environment until use case testing is completed and recorded in source code or configuration change repositories.

6.7.3. Commonwealth Agencies and Offices must ensure that operating systems for email, ***application***, web, database, network devices and file servers are hardened to protect from exploitation from non-authorized or malicious use. Adherence to hardening standards to protect and secure Commonwealth ***information assets*** prior to deployment into production environments is mandatory.

6.7.4. The creation of covert channels or administrative “back doors” in a system and/or ***software*** and its release into the production environment is strictly prohibited. A channel may be considered covert or an administrative “back door” if it allows remote access functionality that was not intended in the ***software*** design specifications.

6.8. Vulnerability Scanning and Patch Management

6.8.1. Commonwealth Agencies and Offices must ensure that ***controls*** are implemented to ensure that the resources, materials, and ***procedures*** used in the development ***process*** are managed to minimize the introduction of security ***vulnerabilities***. In the event of an ***information*** spill or ***data breach***, the Incident Response Plan will be initiated.

6.8.2. Commonwealth Agencies and Offices must ensure that ***information owners*** and/or ***application administrators*** coordinate with their Security Officers and EOTSS' Vulnerability Management Program (VMP) Manager to deploy security ***patches***/updates in a timely fashion to resolve ***vulnerabilities*** while ensuring the full functionality of the ***information system.***

6.8.3. Vendor-supplied ***software*** (e.g., product upgrades, updates, and ***patches***; ***software*** developed by ***third parties***) must be updated and maintained to ensure reduced ***risk*** of security ***vulnerabilities***. Change ***control procedures*** will be documented according to the change and release management *procedures*.

6.8.4. Commonwealth Agencies and Offices will apply the most up-to-date vendor-supplied security ***patches*** or upgrades to correct for known ***vulnerabilities*** in a timely manner.

6.9. Decommissioning

6.9.1. Prior to decommissioning, the ***Information Owner*** will formalize plans that describe the correct, detailed ***processes*** to securely remove, archive, or protect ***sensitive data*** from the systems to be decommissioned.

6.9.2. ***Software*** and/or ***applications*** to be decommissioned must be removed from all enterprise ***assets***.

6.9.3. ***Assets*** containing retired ***software*** must be protected with additional defensive mitigations, such as removal from the network or isolation.

6.9.4. Commonwealth Agencies and Offices should make a copy of the ***user data*** as needed.

6.9.5. The ***information owner*** or ***application administrator*** will ensure that any retired ***software*** did not store ***data*** in other servers or cloud infrastructure not owned by the Commonwealth. This information will be reported to the Vulnerability Management Program (VMP) Director.

7. Roles and Responsibilities

Role	Responsibility
EOTSS Secretary and Commonwealth Chief Information Officer (CIO)	The person responsible for the management, implementation, security and usability of information, technologies, processes, and users within the Commonwealth's IT environment. The Commonwealth CIO has authority over all activities concerning information technology by all Commonwealth Agencies and Offices.
Commonwealth Chief Information Security Officer (CISO)/Chief Risk Officer (CRO)	The person responsible to ensure compliance with this policy across all Commonwealth Agencies and Offices and Agencies. The CISO/CRO leads the ERM Office and is responsible for aligning security initiatives with enterprise programs and business objectives. The CISO/CRO ensures that the Commonwealth's information assets are securely protected.
Chief Technology Officer (CTO)	The person responsible for the management, implementation, security and internal operations of the entire information technology department. The CTO identifies weaknesses and vulnerabilities within the Commonwealth's IT environment and implements controls to protect information assets and reduce risks. The CTO leads technological advancements, determines technology strategy, drives research and develops technology initiatives.
Manager of EOTSS Vulnerability Management Program (VMP)	The person within EOTSS, designated by the Commonwealth CIO to supervise the EOTSS Vulnerability Management Program. As the designee of the Commonwealth CIO, the VMP Manager oversees the vulnerability scanning and penetration testing for all Commonwealth Agencies and Offices. The VMP Manager also receives, and reviews monthly vulnerability scans and decides whether the controls implemented by the agency are sufficient to protect the Commonwealth's information assets and IT systems.
Information Owner	The individual who is responsible for the use and security of specified information, and who is responsible for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner may be designated as the person responsible for the software and/or application(s) in a given agency.

Application Administrator	The individual who manages specific applications or software, including cloud-based applications. Application administrators are in charge of installing, updating, and maintaining their assigned applications. They also troubleshoot concerns, respond to inquiries from application users and manage the relationship with the service provider. The application administrator may be designated as the person responsible for the software and/or application(s) in a given agency.
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, the EOTSS Vulnerability Management Program (VMP) Manager, and/or the ERM office.

8. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Application Management		2.2, 2.3, 2.5, 4.6, 9.7, 10.1, 10.2,	PR.PS-02
Inventories		2.1, 2.4	ID.AM-02
Testing		16.3, 16.4, 16.5	
Risk Assessments		16.6	
Scanning and Patch Management		2.2, 7.6, 7.7, 16.2, 16.5	

9. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Thomas E. McDermott	7/22/2024	Initial Draft
1.1	Miklos Lavicska	8/2/2024	Corrections and Formatting
1.2	Thomas E. McDermott	12/23/2024	Revisions, Corrections and Formatting
1.3	Anthony J. O'Neill	1/1/2025	Final Review
1.4	Thomas E. McDermott	4/4/2025	Updates, Corrections and Formatting
1.4	Miklos Lavicska	4/11/2025	Corrections and Formatting
1.4	Anthony J. O'Neill	4/18/2025	Final Review