Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Enterprise Vulnerability and Risk Management Policy

Document Name: Vulnerability and Risk Management Policy	Effective Date: 1/1/2025
Document ID: IS.010	Last Revised Date: 12/23/2024

Table of Contents

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum security requirements that must be implemented to protect, detect and remediate ***vulnerabilities*** in the Commonwealth's ***information*** technology environment. This ***policy*** reinforces the Commonwealth's commitment to an effective ***vulnerability*** management program and outlines the ***controls*** necessary to safeguard the Commonwealth's ***information assets*** and reduce the ***risks*** posed by ***vulnerabilities*** that may exist in the Commonwealth's IT 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. Additional ***information*** regarding this ***policy*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/***policies***. Definitions of terms in bold may be found in the ***IS Glossary*** 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. ***Exceptions*** to any part of this document must be requested online through ServiceNow, https://www.mass.gov.service-now.com). A ***policy exception*** may be granted only if the benefits of the ***exception*** outweigh the increased ***risks***, as determined by the ***Commonwealth CISO,*** or his or her designee. All ***exceptions*** will be for a limited time and will be narrow in scope.

6. Vulnerability Management

6.1. Commonwealth Agencies and Offices will establish an ongoing ***vulnerability*** and ***patch*** management program for all enterprise ***assets***. The program will include the identification of key ***personnel*** and the assignment of roles and responsibilities.

6.2. Commonwealth Agencies and Offices will designate an ***information owner*** for the ***vulnerability*** and ***patch*** management program.

6.3. The ***information owner*** will serve as the principal point of contact with the EOTSS' Vulnerability Management Program (VMP) and will be responsible for the agency's ***vulnerability*** and ***patch*** management program, including all required scanning, reporting and the implementation of directives issued by EOTSS within established timeframes.

6.4. The ***information owner*** will assist the VMP team with the identification of ***assets*** and ***applications***, and their respective owners.

6.5. The ***information owner*** will be responsible for receiving and acting upon critical ***vulnerability*** advisories issued by EOTSS.

6.6. A ***risk***-based ***vulnerability*** remediation strategy must be utilized to remediate ***vulnerabilities*** and reduce the ***risk*** of identified ***vulnerabilities*** operating within the environment. The ***vulnerability*** remediation strategy will include categorizing ***vulnerabilities*** and establishing remediation timelines based on criticality and ***risk***.

6.7. A defined ***process*** must be in place to monitor ***vulnerability*** reports from ***application*** and ***software*** vendors and evaluate applicability to agency systems.

6.8. Automated ***vulnerability*** scans must be performed on all enterprise ***assets,*** not less than monthly. All ***assets*** and ***applications,*** including those supported by ***third parties***, will be included in the monthly scan, unless the agency has obtained a security ***exception*** from the ***Commonwealth CISO***, or his or her designee.

6.9. Internal scans must include both authenticated and unauthenticated scans using an approved scanning solution, when technically feasible.

6.10. Commonwealth Agencies and Offices will provide monthly reports of all ***vulnerabilities*** identified by the internal scans to the Manager of EOTSS' Vulnerability Management Program (VMP). Reports will include the following:

6.10.1. Existing ***vulnerabilities*** by severity and age

6.10.2. ***Vulnerabilities*** with ***exceptions*** in place

6.10.3. Identification of known false positives

6.10.4. Report of open and closed ***vulnerabilities*** within the last 30 days

6.11. The ***information owner*** will perform a timely review of the ***vulnerability information*** received from internal and external sources and report this ***information*** to the Manager of EOTSS' Vulnerability Management Program (VMP).

6.12. System owners must utilize an automated patching ***process*** whenever technically feasible to apply operating system and ***application*** updates not less than monthly.

6.13. In the event that a ***patch*** or mitigation strategy is not currently available to remediate the ***vulnerability***, the ***vulnerability*** must be formally documented. Commonwealth Agencies and Offices must obtain an ***exception*** as detailed above

before accepting the ***risk***. The ***vulnerability*** must also be added to a POAM, and compensating ***controls*** must be determined.

6.14. Commonwealth Agencies and Offices will conduct penetration testing not less than annually.

6.15. Penetration testing must include internal, ***third-party*** network, and ***application*** layer testing. If penetration testing is not feasible on a ***third-party*** system, then verification of penetration testing from the system provider must be obtained.

6.16. A defined ***process*** for penetration testing finding remediation must be followed that includes categorizing findings and establishing remediation timelines based on criticality and ***risk***.

7. Information Security Risk Management

7.1. The ***Commonwealth CISO*** and CRO will develop a ***process*** and ***risk control*** framework to identify analyze and mitigate ***information security risks*** that could compromise the confidentiality, integrity or availability of the Commonwealth's ***information assets*** and/or systems.

7.2. The ***risk control*** framework will comply with cybersecurity industry best practices, applicable regulatory requirements, and Commonwealth enterprise policies.

7.3. Commonwealth Agencies and Offices will perform an annual identification and analysis of ***information security risks*** that could compromise their enterprise ***assets*** and/or ***information systems***.

7.4. Commonwealth Agencies and Offices will designate a ***risk owner*** and a ***control owner*** to manage the ***risk*** assessment ***process*** and to determine the appropriate ***risk*** treatment.

7.5. The ***risk owner*** and the ***control owner*** will develop a ***risk*** mitigation plan and ensure that specific ***controls*** are implemented that will effectively mitigate identified ***risks***.

7.6. Once identified and properly analyzed, all ***risks*** must be mitigated to an acceptable level to meet organizational ***risk*** tolerance, business objectives and regulatory compliance requirements.

7.7. ***Controls*** that are put in place to mitigate ***risks*** must be evaluated to determine the reduction and impact on the ***residual risk***.

7.8. For ***risks*** outside of the Commonwealth's acceptable levels, a ***risk*** treatment plan must be documented and reported to EOTSS' Office of Enterprise Risk Management (ERM) by the designated owner.

7.9. The ***risk*** treatment plan will include, but not be limited to, the details involved in accepting the ***risk***, mitigating the ***risk*** via implementation of security ***controls***, transferring the ***risk***, or avoiding the ***risk***.

7.10. Commonwealth Agencies and Offices will provide a report of identified ***risks*** annually to the Enterprise Risk Management Office (ERM). The report must include the ***risk*** level (Critical, High, Medium, Low) of each identified ***risk*** and the status of any remediation efforts.

7.11. The identified ***risks*** must also be documented and maintained within a ***risk*** register that includes:

7.11.1. Each potential ***risk's*** impact and likelihood.

7.11.2. The organizational resource cost of mitigating or minimizing the ***risk*** to an acceptable level.

7.11.3. The inherent and residual score for each ***risk***.

7.12. All "Critical" or "High" residual ***risks*** and ***risk*** treatment strategies must be reported to the Commonwealth CRO on a quarterly basis.

8. 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.
Enterprise Risk Management Office	The office within EOTSS responsible for risk strategy, identification, assessment, analysis, monitoring, reporting and mitigation. Under

(ERM)	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.
Chief Technology Officer (CTO)	The person responsible for the management, implementation, security and internal operations of the entire information technology environment. 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. The VMP Manager collaborates with EOTSS leadership to determine whether the controls implemented by the agency are sufficient to protect the Commonwealth's information assets and IT systems.
Information Owner	The individual in each agency who is responsible for the vulnerability and patch management program. The owner serves as the principal point of contact with the EOTSS' Vulnerability Management Program (VMP). The owner is responsible to assist the VMP team with all required scanning and reporting, and to implement directives issued by EOTSS within established timeframes. The owner timely reviews the vulnerability information received from internal and external scans and reports this information to the Manager of EOTSS' VMP Program.
Risk Owner	The individual within an agency or office who is responsible to oversee each individual risk identified in an ERM report. The risk owner serves as an accountable point of contact and is responsible to manage, track and respond to individual risks. The risk owner works with the control owner to develop a risk mitigation plan and ensures that specific controls are implemented that will effectively mitigate identified risks.

Control Owner	The individual within an agency or office who is accountable for implementing and maintaining specific risk mitigation controls. The control owner works with the risk owner to ensure the effectiveness of specific controls within the Commonwealth's information technology (IT) environment.
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 Manager of VMP and/or the ERM office.

9. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Vulnerability Management	RA-05	3.1, 3.6, 3.7, 7.2,16.6, 20.1, 20.2	ID.RA-01, ID.IM-04, PR.PS-02, PR.PS-03,
Information Security Risk Management	PM-9, RA-03, DS-RA-07, CA-07,	-	GV.OC-01, GV.RM-01, GV.RM-03, GV.RM-05, GV.RM-06, GV.PO-01, ID.RA-05, ID.RA-06

10. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/15/2024	Initial Policy Draft
1.1	Thomas E. McDermott	6/25/2024	Revisions, Corrections, and Formatting
1.2	Miklos Lavicska	8/6/2024	Corrections and Formatting
1.3	Thomas E. McDermott	12/23/2024	Revisions, Corrections, and Formatting
1.4	Anthony J. O'Neill	1/1/2025	Final Review