Commonwealth of Massachusetts

Executive Office of Technology Services and Security
Enterprise Risk Management Office

Enterprise Information Security Governance Policy

Document Name: Information Security Governance Policy	Effective Date: 1/1/2025
Document ID: ISP.001	Last Revised Date: 3/25/2025

Table of Contents

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum ***information*** security requirements that must be implemented to protect the Commonwealth's ***information assets.*** This ***policy*** reinforces the Commonwealth's commitment to an effective ***information*** security program, and outlines the framework, principles, and ***controls*** required to ensure the protection of 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. Information Classification

6.1. In order to effectively and consistently manage ***information*** security across the Commonwealth's technology environment, the classification or sensitivity level of all ***information*** must be established. Doing so will ensure that appropriate measures are taken to protect the ***information*** commensurate with its value, and the legal restrictions on its dissemination. The ***Information Custodian*** is responsible for assigning the appropriate classification level. Determining appropriate classification may be based on a combination of source and content (i.e., PII may be ***Restricted*** or ***Confidential*** depending on source). The examples below are not exhaustive lists of all types of ***information***. When ***information*** meets criteria for multiple classifications, it should be classified at the highest level.

6.1.1. ***Restricted*** – Any ***confidential*** or ***personal information*** that is intended for a limited number of people who possess the highest level of access control and security clearance, and who need the ***restricted information*** to perform their duties. ***Restricted information*** is intended for a very limited use and must not be disclosed except to those who have explicit authorization to view or use the ***data***. Unauthorized disclosure of this ***information*** could have a serious adverse impact on the financial, legal, regulatory, or reputational impact on the Commonwealth, its constituents, customers, and business partners.

6.1.2. ***Confidential*** — organization or customer ***information*** that if inappropriately accessed or disclosed could cause adverse financial, legal, regulatory, or reputational damage to the Commonwealth, its constituents, customers, and business partners. Except as required by law, ***confidential information*** must be access-restricted to ***personnel*** who have a business need to access the ***information***. Examples may include but are not limited to:

6.1.2.1. ***Personally identifiable information (PII).***

6.1.2.2. Regulated ***information*** (Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Federal Tax Information (FTI) and other types of ***information***).

6.1.2.3. Employee performance and appraisal documentation.

6.1.2.4. Internal, external, and regulatory audit reports.

6.1.2.5. ***Information*** on the Commonwealth's security posture (e.g., firewall setting.

6.1.2.6. ***information***, security configurations, ***vulnerability*** test reports, breach reports).

6.1.2.7. Passwords or any form of security ***key.***

6.1.3. ***General*** — ***information*** that has NOT been ***published*** and has NOT been expressly authorized for public release but has not been classified as ***confidential*** or ***restricted***. ***General information*** is intended for use within the agency or office. ***General information*** is available to internal ***personnel*** and authorized external parties, (e.g., external audit firms, ***third-party*** vendors, etc.). ***General information*** may be subject to disclosure under Public Records laws Examples may include but are not limited to:

6.1.3.1. Organization charts and ***personnel*** directories.

6.1.3.2. Internal ***policies*** and documentation.

6.1.3.3. ***Personnel*** awareness and training collateral.

6.1.4. ***Published*** — ***information*** that has been expressly approved for public release. ***Information*** can only be designated as ***Published*** by the authorized ***personnel***; each Secretariat is responsible for maintaining the list of authorized ***personnel***. Examples may include but are not limited to:

6.1.4.1. Press releases.

6.1.4.2. ***Information*** on public facing websites (e.g., Mass.gov).

6.1.4.3. Promotional materials for Commonwealth constituent services (e.g., Medicaid enrollment).

6.1.4.4. Advertising of open positions and roles.

7. Information System Classification

7.1. To promote a consistent approach to ***risk*** management, business continuity and disaster recovery, Commonwealth Agencies and Offices will also classify all ***information systems***. ***Information Owners*** are responsible for determining the ***information system*** classification of their ***information system***.

7.2. The classification of an ***information system*** must be based on its most critical component (e.g., where ***information*** is transmitted, processed, or stored).

7.3. Commonwealth Agencies and Offices must conduct a ***business impact analysis*** or a ***risk*** assessment to determine ***information system*** classifications for their ***information assets***.

7.4. ***Information system*** classification must be reviewed at least annually and whenever a significant system change occurs.

8. Information Labeling and Handling

8.1. ***Procedures*** for the handling and labeling of ***information***, both in electronic and physical formats, will be defined and maintained by each Secretariat and will also comply with legal and regulatory obligations.

8.2. All ***information*** which is created, acquired or used in support of Commonwealth business activities, must only be used for its intended business purpose.

8.3. All servers that store any form of Commonwealth ***data*** must be located in the continental United States. Any and all ***third-party*** vendors who provide any type of ***data*** storage, including cloud-based ***data*** storage, ***information*** storage ***applications***, or other cloud-based services, and/or network and ***information*** security management to the Commonwealth, must use servers located in the continental United States to perform these functions and for the storage of Commonwealth ***data***.

8.4. All ***information assets*** must have an ***information owner*** assigned by the respective Commonwealth Agency or Office.

8.5. If for any reason, an agency is unable to determine the classification of the ***information***, the ***information*** will be assigned a higher classification and will be subject to higher ***information*** protection ***controls***.

8.6. ***Data*** loss prevention (DLP) technologies approved or managed by the Enterprise Security Office will be implemented to monitor ***data***-at-rest, ***data***-in-transit, and ***data***-in-use.

8.7. Commonwealth Agencies and Offices will protect ***Information*** in line with its assigned level of classification. Classification levels must be reviewed and updated at least annually.

8.8. Commonwealth Agencies and Offices will limit direct access to ***confidential*** customer ***information*** (e.g., SSN) whenever possible. Access to ***information*** must be limited to those with a need to know, based upon the principle of least privilege.

8.9. Sending Commonwealth ***restricted*** or ***confidential information*** to personal email addresses (e.g., Gmail or Yahoo Mail) is prohibited.

8.10. Protect media containing Commonwealth ***information*** against unauthorized access, misuse, or corruption during transportation.

8.11. Commonwealth Agencies and Offices will by default restrict removable media use by ***personnel***. The use of removable media will be granted only when there is a compelling organizational need, after the agency files a ***policy*** non-compliance report as detailed above.

9. Information Disposal

9.1. Commonwealth Agencies and Offices will establish ***procedures*** for the secure disposal of ***information***. ***Information*** will be retained in accordance with the Massachusetts Statewide Records Retention Schedule, and other applicable laws, executive orders, directives, regulations, ***policies***, ***standards***, guidelines, and operational requirements.

9.2. In order to ensure the secure disposal of Commonwealth ***information***, the ***procedures*** established by Commonwealth Agencies and Offices will include the following:

9.2.1. Sanitize all media to minimize the ***risk*** of ***restricted*** or ***confidential information*** leakage

9.2.2. Log the disposal of ***restricted*** and/or ***confidential information*** to maintain an audit trail

9.2.3. Verify that the ***information assets*** containing any ***restricted*** and/or ***confidential information*** have been removed or securely overwritten prior to ***disposal*** or reuse

9.2.4. Use acceptable industry best practices and standards for ***information*** erasure to ensure ***information*** is unrecoverable.

10. Risk Governance

10.1. The ***Commonwealth CISO***/CRO, or his or her designee, will define organizational objectives and ***risk*** appetite based on known ***risk*** exposure and ***residual risk***.

10.2. The ***Commonwealth CISO***/CRO, or his or her designee, will communicate the organization's cybersecurity ***risk*** posture annually. This will include updating and communicating the Commonwealth's ***risk*** appetite to all relevant ***stakeholders***.

10.3. Commonwealth Agencies and Offices will conduct a security review of all ***third parties*** to identify and govern ***risk*** as part of the procurement process.

10.4. All internal and external ***stakeholders*** are responsible to provide all ***information*** needed to govern ***third-party risk***, as determined by the ***Commonwealth CISO***/CRO, or his or her designee.

11. 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. 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 (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, legal, 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 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.
Security Operations Center (SOC)	The office within EOTSS responsible for monitoring and analyzing the state's security posture, and for detecting, analyzing and responding to cybersecurity incidents. The SOC coordinates with municipal, state, and federal agencies, as well as other stakeholders, in the event of a cybersecurity incident. The SOC is also responsible for communicating any high or critical situations to leadership, and for sharing information and resources as needed, to mitigate the effect of an incident.
Information Custodian	The person responsible for overseeing and implementing the necessary safeguards to protect the information system, at the level classified by the Information Owner (e.g., System Administrator, controlling access to a system component).
Information Owner	The official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
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.

12. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Roles & Responsibilities	PM-14, PM-29	-	GV.OC-02, GV.OV-4
Security Policies, Standards and Procedures	All -1 controls	-	GV.PO-01
Risk Governance	PM-9, RA-3, SR-2, SR-6	15.2	GV.SC-03, GV.RM-01, GV-RM-02,

13. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/20/2024	Initial Policy Draft
1.1	Thomas E. McDermott	8/9/2024	Revisions, Corrections, Formatting
1.2	Miklos Lavicska	9/25/2024	Corrections, 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	3/25/2025	Updates, Corrections, Formatting
1.5	Miklos Lavicska	3/27/25	Corrections, Formatting
1.5	Anthony O'Neill	4/10/2025	Final Review