Commonwealth of Massachusetts
Executive Office of Technology Services and Security
Enterprise Risk Management Office

Enterprise Physical and Environmental Security Policy

Document Name: Physical and Environmental Security Policy	Effective Date: 1/1/2025
Document ID: ISP.007	Last Revised Date: 4/4/2025

Table of Contents

1. Purpose

1.1. Commonwealth Agencies and Offices must ensure that the Commonwealth's ***information assets***, whether on-site or off-site, are protected against unauthorized physical access, damage, or loss due to physical and/or environmental causes. The purpose of this ***policy*** is to establish the minimum security requirements that must be implemented to prevent damage, alteration, and/or destruction of the Commonwealth's ***information*** processing facilities and/or their contents. This document outlines the requirements necessary to safeguard the Commonwealth's ***information*** technology ***assets*** and reduce ***risks*** posed by unauthorized access and/or improper management of the facilities that house those ***assets***.

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. Physical Security

6.1. Commonwealth Agencies and Offices will establish security perimeters to protect facilities that contain Commonwealth ***information*** technology ***assets***. This will include, but may not be limited to, ***information*** processing facilities, ***data*** centers and main or intermediate distribution facilities (MDF or IDF) where core infrastructure is located and where equipment and/or ***data,*** is processed, stored, managed, or transported.

6.2. Commonwealth Agencies and Offices must ensure that physical security for the established security perimeter is clearly defined and outfitted with perimeter protection mechanisms to reduce the ***risk*** of unauthorized access. The level of perimeter protection will be based on the sensitivity and criticality of the ***information asset*** housed and the nature of the supported business functions.

6.3. The following ***controls***, at a minimum, will be considered when implementing and revising perimeter protections, based on business requirements:

6.3.1. Physical barriers, proximity card readers or manned entry points must be in place to control access to internal secured areas to prevent unauthorized entry.

6.3.2. Physical perimeters will be monitored by manual ***controls*** such as security guards and real-time ***controls*** such as remote or live closed-circuit camera consoles.

6.3.3. Physical access to wireless access points, gateways, handheld devices, networking hardware, and telecommunication lines must be restricted to only authorized ***personnel***.

6.3.4. Procedures for secure deliveries from outside entities must be documented. Deliveries in restricted areas must be monitored and recorded.

7. Physical Access

7.1. Commonwealth Agencies and Offices will restrict access to Commonwealth facilities, and internally secured areas, to only authorized ***personnel***. The following are the minimum ***controls*** that must be implemented in order to reduce the ***risk*** of unauthorized access:

7.1.1. All equipment owned or managed by the Commonwealth must reside in facilities with a level of protection that is commensurate with the sensitivity and criticality of the equipment and ***information assets*** (***data*** and equipment) therein.

7.1.2. Physical access ***controls*** (such as card readers and physical barriers) must be implemented for internal, secured areas to prevent unauthorized entry.

7.1.3. All Commonwealth ***personnel*** will be issued a badge to facilitate authorization. Commonwealth Agencies and Offices will establish role-based written procedures for granting, modifying and revoking physical access for both ***personnel*** and visitors.

7.1.4. Access to internally secured areas such as ***data*** centers will be restricted to authorized ***personnel*** with a demonstrated business justification for entering the secured area.

7.1.5. Access to the Badge Administration Console must be restricted to only authorized ***personnel***.

7.1.6. All visitors and maintenance ***personnel*** must enter their ***information*** in a visitor's ***log***, including the time of entry and departure, and be issued a visitor badge or comparable identification to facilitate authorization.

7.1.7. All visitors and maintenance ***personnel*** must notify the Commonwealth of expected visits at least 24 hours prior to arrival. All maintenance ***personnel*** will be escorted by an authorized Commonwealth host who will assume responsibility for being with them at all times while onsite.

7.1.8. All visitor ***logs*** and maintenance ***logs*** must be retained for a specified period of time in compliance with the Commonwealth's record retention schedules, as well as legal, regulatory, and contractual requirements.

8. Environmental Security

8.1. Commonwealth Agencies and Offices will implement ***controls*** to protect Commonwealth facilities, and internally secured areas, against damage from environmental factors (e.g., fire, flood, natural or man-made disasters, power and temperature or humidity variations). Environmental ***controls*** must be sufficient to protect the Commonwealth's ***information assets*** and equipment in owned, rented, and leased facilities.

8.2. Environmental conditions will be monitored. The following are the minimum ***controls*** that must be implemented in order to reduce the ***risk*** of damage from environmental factors:

8.2.1. Continuous monitoring will be performed for fire/smoke in all areas of all facilities. Internal secure areas will be subject to additional monitoring for temperature, water, power continuity, humidity and cleanliness.

8.2.2. To facilitate the detection, suppression, and notification of ***personnel*** in the event of a fire, automatic fire suppression systems and water damage protections will be implemented at all locations where critical or sensitive equipment and ***information*** resides.

8.2.3. Monitoring devices, such as humidity and temperature sensors, must be implemented. These devices must be configured to alert appropriate ***personnel*** when the sensors detect values outside of organization and manufacturer defined tolerances.

8.2.4. Uninterruptable primary and alternate power supplies will be installed where needed to ensure maintenance of the minimum operational capabilities in case of an emergency. Continuous power will be provided for mission-critical ***information assets*** and equipment.

9. Roles and Responsibilities:

Role	Responsibility
Commonwealth Chief Information Security Officer (CISO)/Chief Risk Officer (CRO)	The person responsible to ensure compliance with this policy by 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 IT assets, communication systems, data and technologies are securely protected.

Enterprise Risk Management (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 ensure compliance with applicable laws rules and regulations. ERM works 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 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.
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.

10. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Physical Security	PE-3(3), PS-3(7), PE-4, PE-6(3)	-	PR.AA-06
Physical Access	PE-2(1), PE-2(3), PE-3, PE-20	-	PR.AA-06
Environmental Security	PE-11, PE-13, PE- 14, PE-14(2), PE- 15	-	DE.CM-02

11. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/28/2024	Initial Physical & Environmental Security Policy Draft
1.1	Thomas E. McDermott	12/23/2024	Revisions, Corrections, Formatting
1.2	Anthony J. O'Neill	1/1/2025	Final Review
1.3	Thomas E. McDermott	4/4/2025	Updates, Corrections and Formatting
1.3	Miklos Lavicska	4/11/2025	Corrections and Formatting
1.3	Anthony J. O'Neill	4/18/2025	Final Review