Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Security Office

Physical and Environmental Security Standard

Document Name: Physical and Environmental Security	Effective Date: October 15th, 2018
Document ID: IS.013	Last Revised Date: August 29, 2022

Table of contents

1. PURPOSE

1.1. This ***standard*** establishes requirements prevent damage or physical access to the Commonwealth' s information processing facilities and sensitive data. This standard defines the following controls and acceptable practices:

- Definition of physical security perimeters and required controls
- ***Personnel*** and visitor access controls
- Requirements for environmental protection equipment
- Protection of equipment stored off-site from the Commonwealth's facilities

1.2. Federal statutes and regulations, and, in some cases, state law, may impose security requirements in addition to the security requirements set forth in this ***standard*** (for example, Publication 1075 of the Internal Revenue Service). Nothing in this policy shall be construed or interpreted as contradicting any such federal or state requirement. This ***standard*** is meant to encourage adoption of its security measures as a baseline, in addition to, and not in place of, any other legally required security measures.

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "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, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their ***personnel*** comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this ***standard***.

4.2. The Enterprise Security Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

4.3. Any inquiries or comments regarding this ***standard*** shall be submitted to the Enterprise Security Office by sending an email to EOTSS-DL-Security Office.

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

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to 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 via email to the Security Office (EOTSS-DL-Security Office). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6. STANDARD STATEMENTS

6.1. Facility Control and Secure Areas

Security perimeters shall be defined and established to protect areas that contain sensitive data and critical information processing facilities. This shall include, but may not be limited to, data centers and main or intermediate distribution facilities (MDF or IDF) where core infrastructure is located and where sensitive data is processed, stored, managed or transported.

6.1.1. Physical security perimeters

Commonwealth Offices and Agencies must ensure that physical security for the established security perimeters shall be 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.

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

6.1.1.1. Access control: physical barriers, proximity card readers or manned entry points shall be in place to control access to internal secured areas to prevent unauthorized entry.

6.1.1.2. Site monitoring: physical perimeters shall be monitored by manual controls such as security guards and real-time controls such as remote or live closed-circuit camera consoles.

6.1.2. General access controls

Commonwealth Offices and Agencies shall restrict access to internally secured areas to only authorized ***personnel***. The following are minimum controls for restricting access:

6.1.2.1. Badge assignment process: process for issuing badges, including granting and revoking badges for ***personnel*** and visitors (if applicable) must be documented.

6.1.2.2. Badge system access: access to the badge administration systems must be restricted to only authorized ***personnel***.

6.1.2.3. Authorized ***personnel*** identification: all Commonwealth full-time and part-time ***personnel*** performing services for the Commonwealth shall be issued a badge or

comparable identification. All vendors must provide 24 hours' notice before being on-site.

6.1.2.4. Controlled reception: procedures to securely receive deliveries for restricted areas must be documented. Deliveries for restricted areas shall be monitored and recorded (e.g., delivery company name, time, parcel) for audit purposes.

6.1.2.5. Audit trail of access to restricted areas: the date and time of entry and departure of visitors to areas of IT ***assets*** processing, storing and/or transmitting ***confidential information assets*** shall be recorded and securely maintained (e.g., data centers, server rooms, Department of Revenue).

6.1.2.6. Non-business hours restriction: facility access outside of regular office hours defined by the agency shall be controlled. Access to public areas must be monitored, and access to secure areas must be strictly enforced using the badge and/or escort.

6.1.3. Visitor access control

Commonwealth Offices and Agencies must ensure that visitor access requires additional controls beyond the requirements for general access. The following are minimum controls for restricting visitor access:

6.1.3.1. Visitor sign-in: visitors must sign a visitor's ***log*** that indicates date and time in/out, organization represented (if applicable), and identify the Commonwealth host being visited.

6.1.3.2. Visitor Identification: all visitors shall prominently display their visitor identification (badge or alternate form of identification) at all times while in secured areas (i.e., non-public office areas).

6.1.3.2.1. Visitors without a displayed badge shall be escorted back to the reception area for identification and authorization of access.

6.1.3.2.2. Visitor identification shall be set to expire on the day that the identification is granted.

6.1.3.2.3. If a physical badge is issued, visitors will be asked to surrender the physical badge before leaving the facility or at the date of expiration.

6.1.3.2.4. ***Personnel*** are not allowed to utilize visitor badges.

6.1.3.3. Types of identification: ***personnel*** identification badges shall differ from badges issued to visitors.

6.1.3.4. Positive identification of visitor: visitors must present a government issued, photo identification prior to the issuance of a badge and gaining access to Commonwealth facilities.

6.1.3.5. Visitor Monitoring: within areas that host sensitive information ***assets*** (e.g., data centers), visitors without CORI on file must be monitored at all times by the Commonwealth host.

6.1.3.6. Visitor hosting: the Commonwealth host shall assume responsibility for their visitor for the duration of the visit. Visitors will be granted access to internal secured areas only with authorization.

6.1.4. Security for public, internal and ***personnel*** areas

Commonwealth Offices and Agencies must ensure that all areas that provide access to the Commonwealth network shall implement controls that protect from unauthorized physical access and damage from environmental factors (e.g., fire, flood, natural or man-made disasters, power and temperature or humidity variations).

The following are minimum considerations for securing offices, rooms and facilities:

6.1.4.1. Environment hazards: hazardous and combustible materials shall be stored according to Material Safety Data Sheets (MSDS) to reduce the risk of exposure.

6.1.4.2. Shared facilities: physical and environmental controls shall be sufficient for protecting Commonwealth's information in owned, rented and leased facilities.

6.1.4.3. Health and safety regulation standards: relevant health and safety regulation (e.g., OSHA) standards shall be taken into account to ensure implemented protection controls meet requirements.

6.1.4.4. Physical access to publicly accessible work area outlets: areas accessible to visitors shall not have work area outlets (e.g., Ethernet port) enabled unless network access is explicitly authorized.

6.1.4.5. Physical access to telecommunication equipment: physical access to wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines shall be restricted and/or monitored.

6.1.5. Security for internal secure areas

Secured areas are those used by the Commonwealth to conduct specific security or business-related functions that require the use of ***confidential information***. The following requirements, at a minimum, shall be considered to protect the Commonwealth's secured areas:

6.1.5.1. ***Personnel*** Authorization: access to secured areas such as data centers shall be restricted to authorized ***personnel*** with a demonstrated business justification. Secured areas, where feasible, shall have no obvious signage as to the purpose of the area.

6.1.5.2. Access control mechanisms: secured areas shall be subject to additional entry controls such as locks, proximity card readers and biometric identification.

6.1.5.3. Audit trail: an audit trail of access to secure areas shall be maintained and privileges shall be reviewed regularly to assess validity.

6.2. Equipment and Other Media Security

Commonwealth Offices and Agencies must ensure that the Commonwealth's ***information assets***, whether on-site or off-site, must be protected against unauthorized physical access, damage or loss due to physical and/or environmental causes.

6.2.1 Physical and environmental protection

All equipment owned or managed by the Commonwealth shall be housed in Commonwealth facilities with a level of protection that is commensurate with the sensitivity and criticality of the equipment and the information it handles (see *Asset Management Policy*).

6.2.1.1. Environmental Threats

The potential danger from environmental threats including weather, malicious attacks, and accidents shall be considered and controls appropriate for risk mitigation shall be implemented to reduce the potential for an incident to occur.

Environmental conditions shall be monitored in appropriate areas. At a minimum, monitoring shall be performed for fire/smoke in the general facility areas. Internal secure areas shall be subject to additional monitoring for temperature, water, power continuity, humidity and cleanliness.

Environmental controls such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power and humidity control shall be implemented in facilities in accordance with risk assessments. Data centers shall contain elements of each environmental control at sufficient levels.

6.2.1.2. Backup power

Continuous power shall be provided for mission-critical ***information assets*** through battery-operated uninterrupted power supply (UPS) protection. Consideration for generator backup may be contemplated if risk assessments warrant higher levels of protection.

6.2.1.3. Shutdown procedures

Clearly defined controls and procedures to enable an orderly shutdown of computing resources in the event of a prolonged power failure shall be documented and distributed to the personnel responsible for the shutdown process.

6.2.1.4. Emergency power shutoff

In the case of emergency, emergency power off switches shall be located near emergency exits in equipment rooms to facilitate rapid power down.

6.2.1.5. Alarm systems

Configuration of alarm systems shall be periodically reviewed and evaluated to detect malfunctions in the supporting utilities and reconfigured as needed.

6.2.1.6. Voice services

Telecommunications equipment shall be connected to support redundant connection points to the utility provider to prevent failure in case of emergency. Voice services shall be adequate to meet local legal requirements for emergency communications.

6.2.2. Off-site equipment and security

Equipment (e.g., network and telecommunication devices, servers, power and cooling equipment) may only be taken off-site for valid business reasons and with authorization from the ***Information Owner***.

Individuals taking equipment offsite are responsible for the physical protection of the system and shall ensure the system is secured at all times. Equipment shall be recorded as being removed off-site and recorded when returned as necessary.

6.2.3. Cabling protection

Power and telecommunications cabling shall be protected adequately against risks such as interference, data capture or physical damage. These cables shall be easily identifiable using appropriate markers or labels to ensure handling errors are minimal.

6.2.4. Maintenance of information ***assets***

Equipment maintenance controls, at a minimum, shall include the following:

6.2.4.1. ***Equipment*** shall be serviced in accordance with the manufacturer's/supplier's recommendations and tested periodically.

6.2.4.2. Prior to the disposal or reuse of ***equipment***, all data shall be removed or securely overwritten to ensure that any ***confidential*** data and licensed software is removed (see *Information Disposal in the Asset Management Standard*).

6.2.5. Upon termination of ***personnel*** and/or expiration of external business relationships, all organizationally owned ***equipment*** shall be returned within ten (10) business days.

6.2.6. Workspace security: Food and water shall not be stored around secure areas hosting mission-critical systems (e.g., data centers).

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1 Facility Control and Secure Areas	CP Family	-	-
	PE-1	-	ID.GV-1
	PE-2	-	PR.AC-2
	PE-9	-	ID.BE-4
	PE-10	-	PR.IP-5
	PE-11	-	ID.BE-4
	PE-13	-	PR.IP-5
	PE-15	-	PR.IP-5
	AT-2	CSC 17	PR.AT-1
	AT-3	CSC 5	PR.AT-2
	PL-4	-	-
	PS-6	CSC 13	PR.DS-5
	PE-1	-	ID.GV-1
	PE-2	-	PR.AC-2
	PE-3	-	PR.AC-2
	PE-4	-	PR.AC-2
	PE-6	-	PR.AC-2
	PE-8	-	-
	PE-9	-	ID.BE-4
	PE-11	-	ID.BE-4
	PE-12	-	PR.IP-5
	PE-14	-	PR.IP-5
	PE-16	CSC 1	PR.DS-3
	PE-18	-	PR.IP-5
		-	PR.IP-11
6.2 Equipment and Other Media Security	MA Family	-	-
	MP-5	CSC 8	PR.PT-2
	MP-6	CSC 1	PR.DS-3
	PE-1	-	ID.GV-1
	PE-3	-	PR.AC-2
	PE-6	-	PR.AC-2
	PE-16	CSC 1	PR.DS-3
	PE-19	CSC 13	PR.DS-5
	PE-20	CSC 19	DE.CM-2
	CM-9	CSC 3	PR.IP-1
	PS Family		

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/02/2018	Corrections, Formatting
0.95	Sean Vinck	5/7/2018	Corrections and Formatting
0.96	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-Publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	Annual Review

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement shall be submitted to the document owner.

9.1 Annual Review

This *Physical and Environmental Security Standard* shall be reviewed and updated by the document owner on an annual basis or when significant *Standard* or procedure changes necessitate an amendment.