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

Organization of Information Security Standard

Document Name: Organization of Information Security Standard	Effective Date: October 15th, 2018
Document ID: IS.012	Last Revised Date: March 4, 2025

Table of Contents

1. PURPOSE

1.1. The purpose of this ***standard*** is to:

1.1.1. Protect the Commonwealth's ***information*** by establishing, implementing, and managing ***risk***-based administrative, technical and ***personnel*** safeguards.

1.1.2. Establish responsibility and accountability for ***information*** security in the organization.

1.1.3. Comply with relevant laws, regulations and contractual obligations related to ***information*** security.

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. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in

maintaining and monitoring compliance with this ***standard***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***standard*** 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 ***standard*** 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 ***standard*** and the provisions set forth in any of the Enterprise Information Security Policies, 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. POLICY STATEMENTS

6.1. Information Security Organization Structure

6.1.1. EOTSS's Enterprise Security Office is responsible for information security across the Commonwealth.

6.2. Roles and Responsibilities

6.2.1. The ***information*** security function covers a broad range of activities that touch on multiple organizational facets. In order to effectively and consistently manage ***information*** security across the organization, the following roles and responsibilities are defined and referenced across relevant ***policies*** and ***standards***.

Role	Responsibility
Governance, Risk and Compliance (GRC team)	The executive body responsible for establishing acceptable risk tolerance, ensuring demonstrable alignment of security and business objectives, and reviewing overall direction and priorities for information technology and security policies.
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 standard 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

Role	Responsibility
	implements cybersecurity best practices to mitigate operational, reputational, security and financial risk.
Information Security Team	The team responsible for the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
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).
Personnel	The Commonwealth's state employees, contractors, consultants, vendors, and interns, including full-time, part-time, temporary, or voluntary regardless of rank, position, or title on the Commonwealth payroll.

6.3. Information Security Policy Framework

6.3.1. The Information Security Policy Framework (ISPF) serves as a foundation for the Commonwealth's ***information*** security program and outlines the governance framework that has been adopted by the Commonwealth's leadership to govern ***information*** security across the organization.

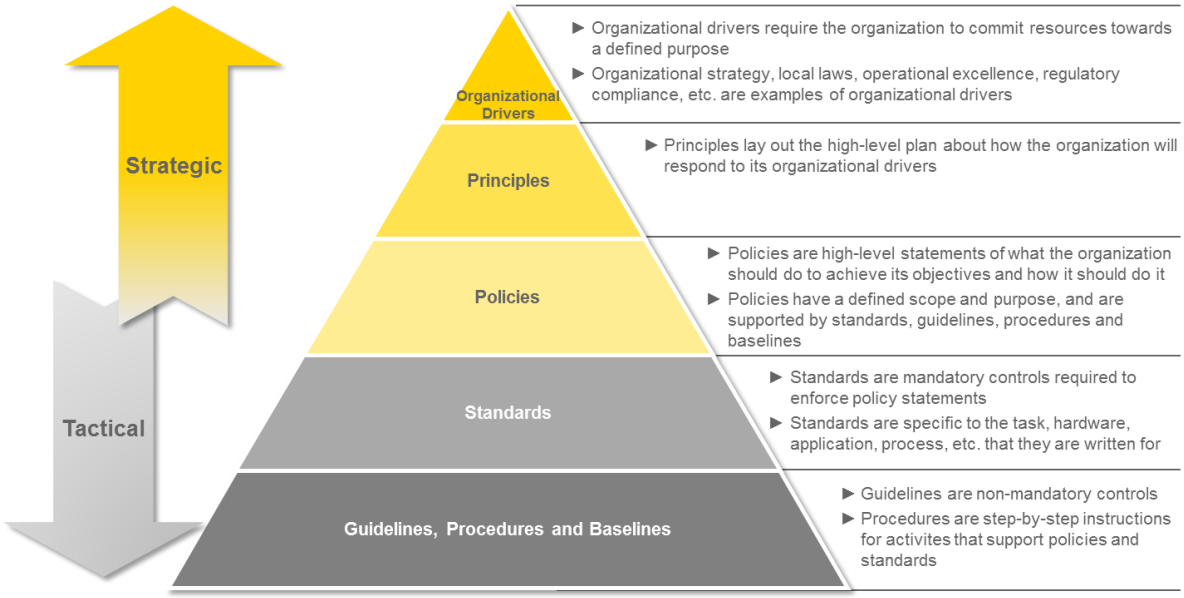

Figure 1 - Information Security Policy Framework (ISPF)

6.3.2. Policy Framework Details

6.3.2.1. The Commonwealth's ISPF consists of the set of ***policies***, ***standards***, ***guidelines*** and ***procedures*** (PSGP). The framework is defined as follows:

6.3.2.1.1. ***Policies*** are mandatory, management statements, instructions or organizational rules that guide behavior and set operational goals. ***Policies*** should be concise and easily understood.

6.3.2.1.2. ***Standards*** are a mandatory set of technical configurations used to ensure that a minimum level of security is provided across multiple implementations of business services, systems, networks and products used throughout the Commonwealth.

6.3.2.1.3. ***Procedures*** contain process-specific operational steps or methods to support the requirements contained in the related ***policy*** and/or ***standard***. Commonwealth Agencies and Offices are encouraged to develop internal ***procedures*** that comply with these ***policies*** and ***standards***.

6.3.2.1.4. ***Guidelines*** are statements that provide optional ***control*** recommendations based on leading best practices.

6.3.2.2. ***Policy*** Areas - The Commonwealth has defined 10 enterprise-level ***information*** security ***policies*** and 17 core enterprise security ***standards***

Policies	Standards
IS.001 Information Security Governance Policy	IS.011 Information Security Standard
IS.002 Acceptable Use of Information Technology Policy	IS.012 Organization of Information Security Standard
IS.003 Access Management Policy	IS.013 Acceptable Use of Information Technology Standard
IS.004 Asset Management Policy	IS.014 Access Management Standard
IS.005 Incident Response Policy	IS.015 Asset Management Standard
IS.006 Change and Configuration Management Policy	IS. 016 Business Continuity and Disaster Recovery Standard
IS.007 Physical and Environmental Security Policy	IS. 017 Communication and Network Security Standard
IS.008 Software and Application Management Policy	IS. 018 Compliance Standard
IS.009 Third Party Risk Management Policy	IS.019 Cryptographic Management Standard
IS.010 Vulnerability and Risk Management Policy	IS.020 Information Security Incident Management Standard
	IS.021 Information Security Risk Management Standard
	IS.022 Logging and Event Monitoring Standard
	IS.023 Operations Management Standard
	IS.024 Physical and Environment Security Standard
	IS.025 Secure System and Software Lifecycle Management Standard
	IS.026 Third Party Information Security Standard
	IS.027 Vulnerability Management Standard

Figure 2 — Information Security Policy Framework

6.4. Policy Life Cycle Management

6.4.1. The Information Security Policy Framework serves to govern the life cycle of the Commonwealth's Information Security PSGPs.

6.4.2. Implementation and compliance monitoring

6.4.2.1. The Enterprise Security Office is responsible for implementing ***procedures*** for monitoring compliance with ***information*** security PSGPs.

6.4.2.2. The Enterprise Security Office will assist agencies to develop tools and enablers to measure their compliance with ***policies*** and ***standards***.

6.4.3. Policy Non-Compliance

6.4.3.1. All Commonwealth Agencies and Offices that receive or expect to receive IT/IS services from the Commonwealth are required to comply with all Enterprise ***Information*** Security ***Policies*** and ***Standards***. All Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel***, including consultants, contractors, and vendors, comply with these requirements.

6.4.3.2. In the event that any Commonwealth Agency, Office, or other party is unable to comply with the requirements of this ***standard***, a policy non-compliance report must be submitted as detailed above.

6.4.3.3. The ERM office, in conjunction with the ***risk*** and ***control*** owners, will evaluate the effectiveness of the ***controls*** in mitigating the identified ***risks*** periodically.

6.4.3.4. Compliance progress will be validated at the expiration date specified in the policy non-compliance report. The ***risk*** mitigation plan established in the non-compliance report may be closed if the agreed-upon solution has been implemented, and the identified ***risks*** have been resolved or mitigated to an acceptable level.

6.4.4. Review Process

6.4.4.1. ***Information*** security PSGPs will be reviewed on a regular basis to ensure they are consistent, practical, and properly address the following:

6.4.4.1.1. Legal, regulatory, and contractual requirements.

6.4.4.1.2. Organizational needs and impact: ***Controls*** remain effective from both a cost and process perspective and support the business without causing unreasonable disruption on the timely execution of those processes.

6.4.4.1.3. Emerging technology environment: Opportunities and threats created by changes, trends and new developments are carefully considered.

6.4.4.1.4. Internal technology environment: Strengths and weaknesses resulting from the Commonwealth's use of technology are considered.

6.4.4.1.5. Other requirements specific to new or unique circumstances are evaluated.

6.4.5. Review intervals

6.4.5.1. A review of ***information*** security ***policies***, ***procedures*** and ***standards*** will be performed by the ***Document Owner***, as follows:

6.4.5.1.1. ***Policies***: Review at least once every year

6.4.5.1.2. ***Standards***: Review at least once every year

6.4.5.1.3. ***Procedures***: Review at least once every year

6.4.5.2. In addition to the defined review cycle, relevant ***information*** security PSGPs will be considered for review and update:

6.4.5.2.1. When a significant change is identified in the technology, business, or regulatory environment that may have a substantial impact on the Commonwealth's ***risk*** posture.

6.4.5.2.2. As part of the post-mortem of ***security incident*** response process.

6.4.5.2.3. After the performance of an internal or external review that identifies a need for change.

6.4.6. Dissemination

6.4.6.1. ***Information*** Security PSGPs will be published and made accessible to the entities covered under the scope of this ***policy***.

6.4.6.2. ***Policies*** and ***standards*** are public documents that are published on the mass.gov web site. ***Guidelines*** and ***Procedures*** contain specific ***information*** about Commonwealth infrastructure and are therefore internal use documents that will only be distributed on a limited basis outside of the Commonwealth.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS Security 20 v6	NIST CSF
6.1 Information Security Organization Structure	PM-1	-	ID.GV-1
	PM-8	-	ID.BE-2
	PM-11	-	ID.AM-6
6.2 Roles and Responsibilities	-	-	-
6.3 Information Security Policy Framework	PM-9	-	ID.GV-4
	PM-15	CSC 4	ID.RA-2
	PM-16	CSC 4	ID.RA-2
	PM-12	-	ID.RA-3

	PM-4	-	ID.RA-6
	PM-13	CSC 17	PR.AT-1
	PM-6	-	PR.IP-7
	PM-14	CSC 19	PR.IP-10
			ID.GV-2
			ID.GV-3
6.4 Information Security Policy Lifecycle Management	AT-2	CSC 17	PR.AT-1
	AT-3	CSC 5	PR.AT-2
	PL-1	-	ID.GV-1
	PL-2	-	PR.IP-7
	PL-3	-	-
	PL-6	-	-
	PL-9	-	-

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.80	Jim Cusson	10/01/2017	Corrections and formatting
0.90	John Merto	12/18/2018	Minor corrections; wording
0.95	Sean Vinck	5/7/2018	Minor Corrections and Formatting
0.96	Andrew Rudder	5/31/2018	Corrections and Formatting
0.97	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	6/1/2018	Final 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	08/22/2022	Annual Review
1.4	Thomas McDermott	10/2/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony O'Neill	10/2/2023	Final Review
1.5	Thomas McDermott	11/4/2024	Corrections, formatting, and Annual Review
1.5	Anthony O'Neill	11/4/2024	Final Review
1.6	Thomas McDermott	2/21/2025	Updates, Corrections and Formatting
1.6	Mikos Lavicska	2/27/2025	Corrections and Formatting
1.6	Anthony O'Neill	3/4/2025	Final Review