



Organization of Information Security Standard

Document Name: Organization of Information Security	Effective Date: October 15 th , 2018
Document ID: IS.001	Last Revised Date: October 2, 2023

Table of contents

1. Purpose	2
2. Authority	2
3. Scope	2
4. Responsibility.....	2
5. Compliance.....	2
6. Policy Statements	3
7. Control Mapping	9
8. Related Documents	9
9. Document Change Control	9

1. PURPOSE

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

- Protect the Commonwealth's business **information** by establishing, implementing, and managing **risk**-based administrative, technical and **personnel** safeguards.
- Establish responsibility and accountability for **information** security in the organization.
- Comply with relevant laws, regulations and contractual obligations related to **information** security.

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 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) such as mass.gov, must agree to comply with this document, with respect to those services, 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**.
- 4.2. The Enterprise Risk Management Office is responsible for the enforcement of compliance with this **standard** and may enlist other offices to assist with the enforcement of this **standard**.
- 4.3. Any inquiries or comments regarding this **standard** must be submitted to the Enterprise Risk Management Office by sending an email to ERM@mass.gov.
- 4.4. Additional **information** regarding this **policy** 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 all state agencies in the Executive Branch including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus, hereinafter referred to as 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. Any and all **exceptions** will be for a specified time and will be narrow in scope.

6. POLICY STATEMENTS

6.1. Information Security Organization Structure

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

6.2. Roles and Responsibilities

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 .
Chief Information Security Officer (CISO)	The person responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that communication systems, confidential information and technologies are adequately protected. The CISO of the Executive Office of Technology Services and Security is the CISO for the Commonwealth of Massachusetts (Commonwealth CISO).
Deputy Chief Information Security Officer (Deputy CISO)	The person responsible for providing advice and support to the CISO and serves as the primary interface with the information security leadership teams of agencies. The Deputy CISO is also responsible for leading the day to day security operations.
EOTSS General Counsel's Office	The persons who are responsible for ensuring compliance with applicable laws, rules, regulations and contractual obligations and will support the regular review process delineated in this policy document.
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 communication systems and confidential information , at the level classified by the Information Owner (e.g., System Administrator, controlling access to a system component).

Role	Responsibility
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

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.

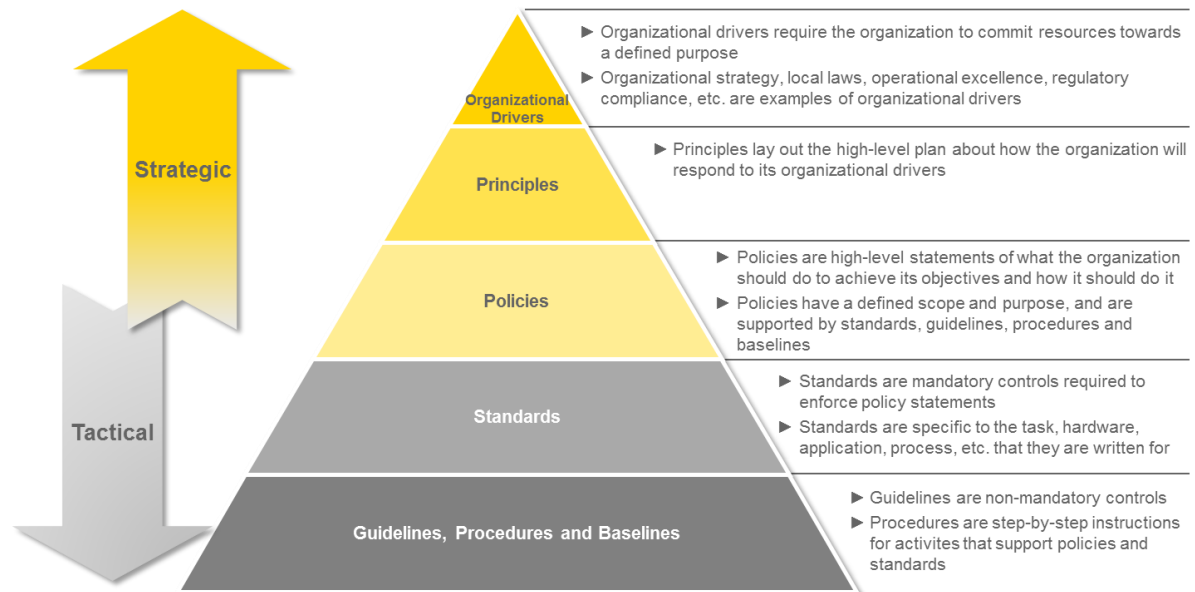


Figure 1 - Information Security Policy Framework (ISPF)

6.3.1. Policy framework details

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

- 6.3.1.1. **Policies** are mandatory, management statements, instructions or organizational rules that guide behavior and set operational goals. **Policies** should be concise and easily understood.
- 6.3.1.2. **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.
- 6.3.1.3. **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**.
- 6.3.1.4. **Guidelines** are statements that provide optional **control** recommendations based on leading best practices.

6.3.1.5. **Policy** Areas

The Commonwealth has defined 1 enterprise-level **information** security **policy**, 1 enterprise acceptable use of **information** technology policy and 15 core enterprise security **standards** as follows:



Figure 2 — Information Security Policy Framework

6.4. Policy Life Cycle Management

The Information Security policy framework serves to govern the life cycle of the Commonwealth's Information Security PSGPs.

6.4.1. Implementation and compliance monitoring

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

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

6.4.2. Policy exceptions

- 6.4.2.1. All Commonwealth Agencies and Offices that receive or expect to receive IT/IS services from the Commonwealth are required to comply with 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.
- 6.4.2.2. In the event that a **policy**, **procedure**, or technical **standard** cannot be adhered to, a **policy exception** request must be submitted online through ServiceNow, <https://www.service-now.com>.
- 6.4.2.3. An **exception** may be granted only if the benefits of the **exception** outweigh the increased **risks** for the approved length of the **exception**, as determined by the **Commonwealth CISO**, or his or her designee, and the associated **Information Owner** or Delegate. Any and all **exceptions** will be for a specified time and will be narrow in scope.
- 6.4.2.4. Compliance progress will be validated at the **exception** expiration date.
- 6.4.2.5. **Exceptions** may be closed if the agreed-upon solution has been implemented and the **exception** has been resolved.
- 6.4.2.6. An extension may be requested if more time is required to implement the long-term solution by completing an extension request.
- 6.4.2.7. Compliance with **policies** and **standards** will be enforced through regular audits by the Enterprise Security Office of Commonwealth Executive Offices and agencies. The Enterprise Security Office will also proffer support if needed to rectify any gaps in the capacity of a Commonwealth entity to ensure compliance.

6.4.3. Additions, changes, and deletions to **policies** and **standards**

- 6.4.3.1. Commonwealth Agencies and Offices may request a new or modification to an enterprise **policy** or **standard** by submitting a change request to the Enterprise Security Office.
- 6.4.3.2. Each request must include the business justification for requesting a change.
- 6.4.3.3. The Enterprise Security Office will review each request and provide recommendations for the **Commonwealth CISO**'s approval or denial.
- 6.4.3.4. The Enterprise Risk Management is responsible for ensuring all approved changes or additions to **information** security **policies** and **standards** are documented and communicated to Commonwealth Agencies and Offices in a timely manner.

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. RELATED DOCUMENTS

Document	Effective date

9. 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 E. McDermott	10/2/2023	Corrections, formatting, updating and Annual Review
1.5	Anthony O'Neill	10/2/2023	Final Review

The owner of this document is the **Commonwealth CISO** (or his or her designee). It is the responsibility of the **document owner** to maintain, update and communicate the content of this document. Questions regarding this document must be submitted to the **document owner** by sending an email to ERM@mass.gov.

9.1 Annual Review

This *Organization of Information Security Standard* will be reviewed and updated by the **document owner** on an annual basis or when significant **policy** or **procedure** changes necessitate an amendment.