# Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

## Information Security Standard

| | |
|---|---|
| Document Name: Information Security Standard | Effective Date: October 15th, 2018 |
| Document ID: IS.011 | Last Revised Date: March 4, 2025 |

### Table of Contents

1. Purpose ........ 2
2. Authority ........ 2
3. Scope ........ 2
4. Responsibility ........ 2
5. Compliance ........ 3
6. Information Security objectives ........ 4
7. Communications ........ 4
8. Reporting requirements ........ 4
9. Requirements ........ 5
10. Standard Framework Coverage ........ 8
11. Document Change Control ........ 10

## 1. PURPOSE

1.1. The purpose of this ***standard*** is to document the framework, principles and controls of an effective ***information*** security program, and outline the ***information*** security requirements to safeguard ***information assets***. The Commonwealth is committed to continually improving the ***information*** security program to meet its strategic objectives and ensure that it is able to adapt to changes in the cyber threat landscape, as well as evolving organizational, legal, and regulatory requirements.

## 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:

5.4. Specifically state the reason/cause of the non-compliance

5.5. Identify and explain in detail the ***risks*** created due to the non-compliance

5.6. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level

5.7. 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.

5.8. 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 SECURITY OBJECTIVES

6.1. The goal of the ***information*** security program is to manage ***risk*** within the Commonwealth's ***information*** technology environment and achieve its ***information*** security objectives through the establishment of supporting ***policies***, ***standards***, ***processes***, and ***controls***. The ***information*** security objectives of the Commonwealth are:

6.2. Enable organizational strategy through the protection of ***data*** and non-public ***information***.

6.2.1. Comply with applicable laws, regulations, and contractual obligations with relevant ***stakeholders***.

6.2.2. Establish a governance structure to effectively and efficiently manage ***information*** security ***risk***.

6.3. Manage identified security ***risks*** to an acceptable (i.e., ***risk tolerance***) level through design, implementation, and maintenance ***risk*** remediation plans.

6.4. Establish a culture of accountability and increasing the level of awareness of all ***personnel*** in order to meet ***information*** security requirements.

6.5. Establish responsibility and accountability for ***information*** security ***policies, standards*** and governance across the Commonwealth.

## 7. COMMUNICATIONS

7.1. The Commonwealth's Information Security ***policies*** and ***standards*** are publicly available on the mass.gov website. EOTSS will inform Commonwealth agencies when ***policies*** or ***standards*** are created, or when major revisions are published.

## 8. REPORTING REQUIREMENTS

8.1. Violations

8.1.1. Compliance with this document is mandatory for all Commonwealth Agencies and Offices. Violation of the requirements of this ***standard*** may cause irreparable injury to the Commonwealth of Massachusetts. 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.

8.2. Reporting Violations

8.2.1. Any violation of the security requirements of this ***standard*** should be reported to agency management and/or the ***Information Security Team***.

***Information*** security ***incidents*** (e.g., ***security breaches***) will follow the reporting requirements outlined in *IS.020 Information Security Incident Management Standard*.

8.3. Information Security Policy Non-Compliance Reports

8.3.1. In the event that any Commonwealth Agency, Office, or other party is unable to comply with the requirements of this ***standard***, an Information Security Policy Non-Compliance Report must be submitted as detailed above.

## 9. REQUIREMENTS

9.1. Organization of Information Security

9.1.1. Commonwealth Agencies and Offices will develop, maintain, and implement ***policies***, ***standards***, ***guidelines***, and ***procedures*** (PSGPs) to support the Commonwealth's ***information*** security program to safeguard the confidentiality, integrity, and availability of its ***information assets***, as directed by the Commonwealth's technology leadership.

9.2. Acceptable Use

9.2.1. ***Personnel*** are the first line of defense and have a shared responsibility to safeguard ***information*** owned or entrusted to the Commonwealth.

9.3. Access Management

9.3.1. Access will be managed throughout the account lifecycle from the initial identification of a ***user*** to the granting, modifying, and revoking of ***user*** access privileges to confirm that ***information assets*** are protected from unauthorized access.

9.3.2. Accounts will be provisioned using the principle of least privilege.

9.3.3. Access privileges will be monitored and reviewed periodically commensurate with their ***risk*** classification.

9.3.4. Passwords must meet the Commonwealth's complexity requirements and should be changed on a regular basis.

9.4. Asset Management

9.4.1. Agencies will establish and maintain an ***asset*** inventory and implement a program to manage the ***asset*** life cycle (i.e., procurement through end-of-support/end-of-life).

9.4.2. Agencies will implement security ***controls*** to protect ***endpoints*** and mobile devices from ***malware*** and ***information*** leakage.

9.5. Business Continuity and Disaster Recovery

9.5.1. Commonwealth Agencies and Offices must protect mission-critical ***information assets***, processes, and facilities from the effects of major failures or disasters by developing and implementing a business continuity strategy that is consistent with organizational objectives and priorities.

9.5.2. Commonwealth Agencies and Offices are required to back up critical ***data***, such as ***confidential information***, and strive to prevent disasters and implement timely recovery from disasters as well as continue critical organizational functions during a disaster or major disruption while maintaining confidentiality.

9.6. Communication and Network Security Management

9.6.1. Commonwealth Agencies and Offices will implement network security ***controls*** such as firewalls, intrusion prevention/detection systems (IPS/IDS), virtual private networks (VPNs) and segmentation techniques so that the Commonwealth protects its ***information assets*** from compromise both from external and internal actors.

9.7. Compliance

9.7.1. Commonwealth Agencies and Offices will establish a compliance framework that will enable the Commonwealth to comply with all relevant legislative, regulatory, statutory, and contractual requirements related to ***information*** security.

9.8. Cryptographic Management

9.8.1. Define requirements for encrypting ***data*** at rest, ***data*** in transit and ***data*** in use, commensurate with the ***information*** classification of the ***information*** requiring protection. Maintain ***cryptographic keys*** to preserve the integrity of cryptographic ***controls***. Use of ***encryption controls*** will be determined after a ***risk*** assessment is performed.

9.9. Information Security Incident Management

9.9.1. Commonwealth Agencies and Offices will develop, maintain, and implement ***policies***, ***standards***, ***guidelines***, and ***procedures*** (PSGPs) to effectively detect, respond and resolve incidents that affect the security of the Commonwealth's ***information assets***, including establishing a Security Incident Response Team (SIRT) to manage the incident response process.

9.9.2. PSGPs will identify relevant stakeholders (both internal and external).

9.9.3. Commonwealth Agencies and Offices will test incident response plans not less than annually.

9.10. Information Security Risk Management

9.10.1. Commonwealth Agencies and Offices will identify and analyze ***information*** security ***risks*** that could compromise the confidentiality, integrity, or availability of the Commonwealth's ***information assets***, and mitigate them to an acceptable level to meet organizational objectives and compliance requirements.

9.10.2. All relevant statutory, regulatory, and contractual requirements that include security and privacy ***controls***, and the Commonwealth's approach to meet these requirements must be explicitly defined, documented, and kept up to date.

9.11. Logging and Event Monitoring

9.11.1. Commonwealth Agencies and Offices will develop and implement a ***process*** to monitor and review activity on ***information systems***, so that ***information system*** problems are identified and corrected, and operator ***logs***, and fault logging are enabled, collected, and reviewed.

9.11.2. The Commonwealth must comply with all relevant legal, regulatory, and contractual requirements applicable to logging and ***event*** monitoring.

9.12. Operations Management

9.12.1. Agencies and Offices will develop and document standard operating ***procedures***, change management, configuration management, capacity management and release management ***processes*** for technology environments.

9.12.2. Agencies and Offices will back up ***information*** in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

9.12.3. Agencies and Offices will establish ***standards*** to support the secure implementation of ***applications*** and services in public and private cloud environments, including ***Software*** as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

9.13. Physical and Environment Security

9.13.1. Commonwealth Agencies and Offices will enforce physical security ***controls*** to manage access to ***information assets***.

9.13.2. Organizations must physically protect facilities with safeguards to protect ***information assets*** against environmental hazards.

9.14. Secure System and Software Life Cycle Management

9.14.1. Commonwealth Agencies and Offices will perform ***information*** security reviews throughout all phases of the system and ***software*** management lifecycle to ensure ***risks*** are properly identified, addressed, and mitigated in a timely and cost-efficient manner.

9.14.2. Agencies and Offices must configure systems using security hardening standards and review configurations periodically.

9.15. Third-party Information Security

9.15.1. Commonwealth Agencies and Offices will establish a process to perform initial ***risk*** assessments and perform ongoing due diligence of ***third parties*** that enter formal business arrangements with the Commonwealth.

9.15.2. Contractual agreements between ***third parties*** and Commonwealth agencies must address baseline ***information*** security clauses, including, but not limited to, the right to audit and adhere to ***data*** protection requirements.

9.16. Vulnerability Management

9.16.1. Commonwealth Agencies and Offices must implement security ***controls*** to manage and monitor ***risks*** to the Commonwealth's ***information*** technology environment.

9.16.2. ***Vulnerability*** management ***personnel*** must be able to identify and respond to ***vulnerabilities*** within established and predictable timeframes.

9.16.3. ***Vulnerability*** management activities must be reported to management on a regular basis.

## 10. STANDARD FRAMEWORK COVERAGE

| Standard ref. | Standard name | Topics covered |
|---|---|---|
| IS.012 | Organization of Information Security Standard | • Information Security Organization Structure<br>• Roles and Responsibilities<br>• Standard Framework<br>• Standard Life Cycle Management |
| IS.013 | Acceptable Use of Information Technology Standard | |

| **Standard ref.** | **Standard name** | **Topics covered** |
|---|---|---|
| IS.014 | Access Management Standard | • User and System Access Management<br>• Account Management<br>• Password Management |
| IS.015 | Asset Management Standard | • Information Asset Management<br>• Information Protection Requirements<br>• Information Classification<br>• Information System Classification<br>• Information Labeling and Handling<br>• Endpoint Security<br>• Information Disposal<br>• Mobile Device Management |
| IS.016 | Business Continuity and Disaster Recovery Standard | • Business Continuity<br>• Disaster Recovery |
| IS.017 | Communication and Network Security Standard | • Network Security Management<br>• Remote Access Security Management<br>• Secure File Transfer<br>• Management of Third-party Network Access |
| IS.018 | Compliance Standard | • Compliance with Policies, Standards, Guidelines, and Procedures<br>• Reporting Security Incidents and Violations<br>• Security Compliance Reviews<br>• External Attestation of Compliance |
| IS.019 | Cryptographic Management Standard | • Key Management<br>• Approved Cryptography Techniques |
| IS.020 | Information Security Incident Management Standard | • Information Security Incident Management |
| IS.021 | Information Security Risk Management Standard | • Information Security Risk Management<br>• Security Awareness and Training |
| IS.022 | Logging and Event Monitoring Standard | • Logging and Event Monitoring |
| IS.023 | Operations Management Standard | • Standard Operating Procedures<br>• Change Management<br>• Configuration Management<br>• Capacity Management<br>• Release Management<br>• Data Backup and Restoration<br>• Cloud Computing |

| Standard ref. | Standard name | Topics covered |
|---|---|---|
| IS.024 | Physical and Environmental Security Standard | • Facility Controls and Secure Areas<br>• Equipment and Other Media Security |
| IS.025 | Secure System and Software Lifecycle Management Standard | • Security in System and Software Life Cycle<br>• Security in SDLC Support Processes<br>• System Hardening |
| IS.026 | Third Party Information Security Standard | • Contractual Security Risk Identification<br>• Third-party Selection<br>• Contractual Security Provisions<br>• Third-party Life Cycle Management |
| IS.027 | Vulnerability Management Standard | • Vulnerability and Patch Management |

Table 1 — Standard Structure

## 11. 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 | 12/18/2017 | 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 | 06/01/2018 | Final 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 |
| 1.4 | Thomas McDermott | 9/27/2023 | Annual Review, Corrections and Updating |
| 1.4 | Anthony O’Neill | 9/27/2023 | Final Review |
| 1.5 | Thomas McDermott | 11/4/2024 | Annual Review, Corrections and Formatting |
| 1.5 | Anthony O’Neill | 11/4/2024 | Final Review |
| 1.6 | Thomas McDermott | 2/4/2025 | Updates, Corrections and Formatting |

| | | | |
|---|---|---|---|
| 1.6 | Miklos Lavicska | 2/27/2025 | Corrections and Formatting |
| 1.6 | Anthony O’Neill | 3/4/2025 | Final Review |