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

Enterprise Information Security Policy

Document Name: Enterprise Information Security	Effective Date: October 15th, 2018
Document ID: IS.000	Last Revised Date: November 04, 2021

Table of contents

1. PURPOSE

1.1. The Commonwealth of Massachusetts. ("the Commonwealth") collects, manages, and stores information on a regular basis in order to support business operations. The Commonwealth is committed to preserving the confidentiality, integrity, and availability of its ***information assets****.

The Commonwealth must protect its information assets, provide for the integrity of business processes and records, and comply with applicable laws and regulations.

This document, the Enterprise *Information Security Policy* (hereafter, the "Policy"), reinforces Leadership's commitment, establishes high-level functions of an information security program, and outlines information security requirements to safeguard *information assets* and assist the Commonwealth to achieve its strategic objectives.

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 (EOTSS) 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 all state agencies in the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices within an executive office. 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, with respect to those services, as a condition of use.

4. RESPONSIBILITY

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

4.2. The Enterprise Security Office is responsible for compliance with this policy and may enlist other departments in the maintaining and monitoring compliance with this *policy*.

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 document and its related policy and standards can be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1 Compliance with this document is mandatory. 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.

6. INFORMATION SECURITY OBJECTIVES

The goal of the Information Security Program is to manage risk within the Commonwealth and achieve its information security objectives through the establishment of supporting policies, processes, and functions. The information security objectives of the Commonwealth are:

6.1 Enable organizational strategy through the protection of customer data and material non-public information.

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

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

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

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

6.6 Establish responsibility and accountability for information security policies and governance across the Commonwealth.

The Commonwealth is committed to continually improving the Information Security Program to help ensure that its applicable information security objectives are met and it is able to adapt to changes in the cyber threat landscape and account for evolving organizational, legal and regulatory requirements.

7. COMMUNICATIONS

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

8. REPORTING REQUIREMENTS

8.1 Policy Violations

Compliance with this document is mandatory for all state agencies in the Executive Department. Violation of this document 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 of Policy Violations

Any violation of this policy should be reported to a supervisor and/or the Information Security Team. Information security incidents (e.g., security breaches) shall follow the reporting requirements outlined in the *Information Security Incident Management Standard.*

8.3 Exceptions from Policy

The policy applies to all state agencies in the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices within an executive office. In the event that a policy or procedure cannot be adhered to, a policy exception request must be submitted to and approved by the Commonwealth CISO, Deputy CISO, or delegate.

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 and the associated ***Information Owner***. Compliance progress shall be validated at the exception expiration date. Exceptions may be closed if the agreed-upon solution has been implemented and the exception has been resolved. An extension may be requested if more time is required to implement the long-term solution by completing an extension request.

9. POLICY STATEMENTS

9.1 Organization of Information Security

Each organization subject to these policies shall develop, maintain and implement policies, procedures, guidelines, and standards (PSGPs) to establish and govern 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

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

Access shall 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. Accounts shall be provisioned using the least privilege access principle. Access privileges shall be monitored and reviewed periodically commensurate with their risk

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

9.4 Asset Management

Establish an information system classification schema to promote a consistent approach to risk management, business continuity and disaster recovery for information assets. Maintain an asset inventory and establish a program to manage the asset life cycle (i.e., procurement through end-of-support/end-of-life). Implement security controls to protect endpoints and mobile devices from malware and information leakage.

9.5 Business Continuity and Disaster Recovery

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. 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

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

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

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 shall be determined after a risk assessment has been performed.

9.9 Information Security Incident Management

Establish a program 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. Develop incident response procedures/plans and identify relevant stakeholders (both internal and external). Test incident response plans periodically for relevancy.

9.10 Information Security Risk Management

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. 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

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

9.12 Operations Management

Develop and document standard operating procedures, change management, configuration management, capacity management and release management processes for technology environments. Back up information in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

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

Enforce physical security controls to manage access to ***information assets***. Physically protect facilities with safeguards to protect ***information assets*** against environmental hazards.

9.14 Secure System and Software Life Cycle Management

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. Configure systems using security hardening standards and review configurations periodically.

9.15 Third-party Information Security

Establish a process to perform initial and ongoing due diligence of third parties that enter into formal business arrangements with Commonwealth agencies. 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

Implement security controls to manage and monitor risks to the Commonwealth's information technology environment. Vulnerability management personnel must be able to identify and respond to vulnerabilities within established and predictable timeframes. Vulnerability management activities must be reported to management periodically.

10. POLICY FRAMEWORK COVERAGE

Policy ref.	Policy/Standard name	Topics covered
IS 001	Organization of Information Security	• Information Security Organization Structure • Roles and Responsibilities • Policy Framework • Policy Life Cycle Management
IS 002	Acceptable Use of Information Technology	
IS 003	Access Management	• User and System Access Management • Account Management • Password Management

Policy ref.	Policy/Standard name	Topics covered
IS 004	Asset Management	• Information Asset Management • Information Protection Requirements • Information Classification • Information System Classification • Information Labeling and Handling • Endpoint Security • Information Disposal • Mobile Device Management
IS 005	Business Continuity and Disaster Recovery	• Business Continuity • Disaster Recovery
IS 006	Communication and Network Security	• Network Security Management • Remote Access Security Management • Secure File Transfer • Management of Third-party Network Access
IS 007	Compliance	• Compliance with Policies, Standards, Guidelines, and Procedures • Reporting Security Incidents and Violations • Security Compliance Reviews • External Attestation of Compliance
IS 008	Cryptographic Management	• Key Management • Approved Cryptography Techniques
IS 009	Information Security Incident Management	• Information Security Incident Management
IS 010	Information Security Risk Management	• Information Security Risk Management • Security Awareness and Training
IS 011	Logging and Event Monitoring	• Logging and Event Monitoring
IS 012	Operations Management	• Standard Operating Procedures • Change Management • Configuration Management • Capacity Management • Release Management • Data Backup and Restoration • Cloud Computing
IS 013	Physical and Environment Security	• Facility Controls and Secure Areas • Equipment and Other Media Security
IS 014	Secure System and Software Lifecycle Management	• Security in System and Software Life Cycle • Security in SDLC Support Processes • System Hardening
IS 015	Third Party Information Security	• Contractual Security Risk Identification • Third-party Selection • Contractual Security Provisions • Third-party Life Cycle Management
IS 016	Vulnerability Management	• Vulnerability and Patch Management
N/A	Glossary of Terms	N/A

Table 1 — Policy 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	5.7.18	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

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 must be submitted to the document owner.

11.1 Annual Review

This *Enterprise Information Security Policy* must be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.