Commonwealth of Massachusetts

Executive Office of Technology Services and Security
Enterprise Risk Management Office

Enterprise Acceptable Use of Information Technology Policy

Document Name: Acceptable Use of Information Technology Policy	Effective Date: 1/1/2025
Document ID: ISP.002	Last Revised Date: 4/11/2025

Table of Contents

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum security requirements that must be implemented to protect the Commonwealth's ***information*** and technology ***assets*** and ensure the continuous effective and secure management of the Commonwealth's ***information*** technology environment.

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. Responsibilities

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***policy***. The Enterprise Risk Management Office is responsible for this ***policy*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***policy***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***policy*** 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 ***policy*** 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 ***policy*** and the provisions set forth in any of the Enterprise Information Security Standards, 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 timeframe 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. Requirements

6.1. Information Security Awareness and Training

6.1.1. ***Personnel*** will review, acknowledge, and agree to comply with security awareness policy through the completion of annually required employee training that helps protect Commonwealth ***information assets*.**

6.1.2. ***Personnel*** will acknowledge completion of security awareness training and agree to comply with this ***policy***.

6.1.3. Commonwealth Agencies and Offices will provide additional security awareness training for job functions that require it in order to obtain additional access agreements.

6.1.4. Completion of the training provided will be tracked and monitored by EOTSS on an annual basis.

6.1.5. EOTSS will suggest and approve security training content. The Human Resources Division (HRD) of the Executive Office for Administration and Finance will be responsible to distribute statewide required training programs for Commonwealth Executive Branch ***personnel*** consistent with this ***policy***.

6.1.6. Commonwealth Agencies and Offices will ensure that all their ***personnel*** complete the required statewide cybersecurity training annually, or as assigned by HRD.

6.2. Acceptable Use of Information Assets

6.2.1. Commonwealth Agencies and Offices will require their ***personnel*** to comply with their applicable ***Code of Conduct***, as well as all enterprise and agency- level ***policies*** and/or applicable contractual obligations.

6.2.2. ***Users*** are permitted to use State Government Systems for official business purposes only. Any unauthorized use is strictly prohibited.

6.2.3. ***Users*** must comply with all applicable laws, regulations, and policies governing the use of ***information*** technology resources.

6.2.4. ***Users*** are responsible for safeguarding ***sensitive information*** and preventing unauthorized access, disclosure, or alteration of ***data***.

6.2.5. ***Information*** security ***controls*** placed on Commonwealth-issued devices must not be circumvented.

6.2.6. ***Users*** should use Commonwealth Systems efficiently and refrain from activities that could degrade system performance or consume excessive network bandwidth.

6.2.7. ***Users*** must respect the rights and privacy of others and refrain from engaging in activities that are harassing, defamatory, or otherwise inappropriate.

6.2.8. ***Users*** must report any suspected security ***incidents*** or breaches to the designated authority promptly.

6.3. Unacceptable Use of Information Assets

6.3.1. It is unacceptable for ***personnel*** to use agency ***information*** technology resources for any of the following:

6.3.1.1 In furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal.

6.3.1.2. For any political purpose.

6.3.1.3. For any commercial purpose.

6.3.1.4. To send threatening or harassing messages, whether sexual or otherwise.

6.3.1.5. To access or share sexually explicit, obscene, or otherwise inappropriate materials.

6.3.1.6. To infringe any intellectual property rights.

6.3.1.7. To gain, or attempt to gain, unauthorized access to any computer or network.

6.3.1.8. For any use that causes interference with or disruption of network ***users*** and resources, including propagation of computer viruses or other harmful programs.

6.3.1.9. To intercept communications intended for other persons.

6.3.1.10. To misrepresent either the agency or a person's role at the agency.

6.3.1.11. To distribute chain letters.

6.3.1.12. To libel or otherwise defame any person.

6.4. Email Use

6.4.1. The following instructions are designed to prevent ***personnel*** from engaging in harmful email practices:

6.4.1.1. Do not use email accounts for any personal purpose, and/or any commercial purposes unrelated to Commonwealth business.

6.4.1.2. Do not conduct government business through or send ***confidential information*** to a personal email account. For purposes of this section, conducting government business prohibits the automatic forwarding of email to a personal email account, using a personal email account as a substitute for a Commonwealth email account, and/or using any email ***application*** in place of the email ***application*** provided by the Commonwealth, to conduct government business.

6.4.1.3. Do not send ***confidential information*** to any recipient not authorized to receive such ***information***. For purposes of this section, a "recipient" includes sending such email to the employee's personal email account.

6.4.1.4. Do not use email to transmit ***confidential information*** in an unencrypted format.

6.4.1.5. Do not collect and/or transmit material in violation of any federal, state, or local law or organizational ***policy***.

6.4.1.6. Do not change the settings of a Commonwealth email account to automatically forward work email to a personal email account.

6.4.1.7. ***Users*** will not use email to misrepresent either the agency or a person's role at the agency.

6.4.1.8. ***Users*** will not use email to distribute chain letters.

6.4.1.9. ***Users*** will not use email to libel or otherwise defame any person.

6.5. Use of Technology Assets

6.5.1. ***Personnel*** must use the Commonwealth's technology ***assets*** appropriately and comply with the following requirements:

6.5.1.1. Do not download or install unauthorized (e.g., unlicensed, pirated) ***software*** onto Commonwealth-issued devices.

6.5.1.2. Avoid using system ***information*** technology resources for personal use, including but not limited to network capacity (e.g., high use of

video streaming technologies).

6.5.1.3. Commonwealth Agencies and Offices must ensure that their ***personnel*** understand that Commonwealth ***information*** technology resources and Commonwealth-issued devices are distributed to ***personnel*** for the purpose of helping them perform their official duties and are not for their personal use.

6.5.1.4. Do not circumvent, attempt to circumvent, or assist another individual in circumventing the ***information*** security ***controls*** in place to protect Commonwealth-issued devices.

6.5.1.5. ***Users*** will not use personal devices to conduct Commonwealth business unless they have obtained prior approval from management.

6.6. Secure Transfer and Control of Information

6.6.1. ***Restricted*** and/or ***Confidential Information*** will be securely exchanged through only authorized methods.

6.6.2. ***Restricted*** and/or ***Confidential Information*** will not be electronically transferred in an unencrypted or unprotected format.

6.6.3. Record Retention timeframes and ***information*** storage will be limited to those required for legal, regulatory, and business purposes.

6.6.4. ***Personnel*** must keep their assigned workspace secure, (e.g., lock ***restricted*** and/or ***confidential information*** in drawers, use cable locks if issued by the Commonwealth).

6.6.5. ***Personnel*** must be careful when using mobile devices (e.g., smartphones and tablets) with access to Commonwealth ***information***. Mobile devices must be secured with a password that meets or exceeds the ***access control*** requirements and must not be left unattended.

6.6.6. When ***personnel*** are telecommuting or working remotely, Commonwealth- owned devices must not be left unattended in public spaces, such as on public transportation, in a restaurant or coffee shop, or in a doctor's office.

6.6.7. Documents containing ***confidential information*** that are sent to a shared printer must be retrieved immediately to reduce the ***risk*** of unauthorized access.

6.7. Privacy and Monitoring

6.7.1. The use of Commonwealth-owned and Commonwealth-issued ***information*** systems and ***assets*** is subject to monitoring and review.

6.7.2. ***Personnel*** should have no expectation of privacy with respect to the Commonwealth's communications systems.

6.7.3. The Commonwealth's communications systems (e.g., emails, instant messages, Internet usage) may be monitored, logged, reviewed, recorded and/or investigated.

6.7.4. Records of activity on these systems may be used by the Commonwealth and/or turned over to law enforcement authorities and other ***third parties***.

6.7.5. ***Personnel*** must be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic.

6.7.6. Commonwealth Agencies and Offices retain, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, will exercise the right to inspect any ***user's*** computer, Commonwealth-issued laptop, phone, or other Commonwealth- issued or managed device, and any ***information*** contained in, accessed by, and/or any ***information*** sent or received by the ***user's*** computer, Commonwealth-issued laptop, phone, or other Commonwealth-issued or managed device.

6.7.7. ***Users*** that voluntarily choose to use their personal mobile devices for Commonwealth business must acknowledge in writing that they understand the ***risks*** of using their mobiles devices, including the potential ***risk*** that their mobile devices will be subject to search and/or inspection, and that they must adhere to Commonwealth ***policies*** and ***standards***.

6.8. Information Protection

6.8.1. All Commonwealth Agencies and Offices must ensure that ***personnel*** adhere to the following requirements for ***Information*** Protection:

6.8.2. ***Personnel*** must adhere to the Commonwealth's ***information*** classification system and ensure that appropriate measures are taken to protect ***information*** commensurate with its value to the Commonwealth. The ***information*** classification system includes ***Restricted Information***, ***Confidential Information, General*** and ***Published Information.***

6.8.3. The confidentiality and integrity of ***information*** must be protected at rest, in use and in transit.

7. Roles and Responsibilities

Role	Responsibility
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 for ensuring compliance with this policy across all Commonwealth Agencies and Offices and Agencies. 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 implements cybersecurity best practices to mitigate operational, reputational, security and financial risk.
Chief Technology Officer (CTO)	The person responsible for the management, implementation, security and internal operations of the entire information technology environment. The CTO identifies weaknesses and vulnerabilities within the Commonwealth's IT environment and implements controls to protect information assets and reduce risks. The CTO leads technological advancements, determines technology strategy, drives research and develops technology initiatives.
Human Resources Division (HRD)	The agency within the Executive Office for Administration and Finance responsible for creating training programs for Commonwealth Executive Branch personnel. HRD is responsible for delivering annual security training to personnel under the subject matter guidance of EOTSS.

Commonwealth Agencies and Offices	Commonwealth Agencies and Offices are responsible for adhering to this policy and complying with the requirements in this document in addition to any supporting documentation issued by the Secretary of EOTSS/Commonwealth CIO, the Commonwealth CISO/CRO, and/or the ERM office. Commonwealth Agencies and Offices are responsible for ensuring that all of their personnel complete annual cybersecurity training, or as assigned by HRD.

8. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Information Security Awareness and Training		14.1, 14.9	GV.RR-01, GV.RR-02, PR.AT-01, PR.AT-02,
Secure Transfer and Control of Information		3.1, 3.4, 3.6	ID.AM-07
Acceptable Use	PL-4, PS-6		PR.AT

9. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/24/2024	Initial Acceptable Use Policy Draft
1.1	Thomas E. McDermott	12/23/2024	Revisions, Corrections, and Formatting
1.2	Anthony J. O'Neill	1/1/2025	Final Review
1.3	Thomas E. McDermott	3/26/2025	Updates, Corrections and Formatting
1.3	Miklos Lavicska	3/28/2025	Corrections and Formatting
1.3	Anthony J. O'Neill	4/11/2025	Final Review