Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Acceptable Use of Information Technology Standard

Document Name: Acceptable Use of Information Technology Standard Document ID: IS.013	Effective Date: October 15th, 2018 Last Revised Date: March 4, 2025

Table of Contents

1. Purpose

1.1. The purpose of this ***standard*** 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. This standard documents the responsibilities of all Commonwealth Agencies and Offices to safeguard both the ***information*** and technology ***assets*** owned or entrusted to the Commonwealth.

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. Requirements

6.1. Information Security Awareness Training - The Commonwealth is committed to establishing an ***information*** security-aware culture to help protect its ***information assets***. To support this goal, the Commonwealth has established the following practices:

6.1.1 New Hires:

All new hires must complete security awareness training within the established new hire training timeline and regularly thereafter. Employees will acknowledge and agree to the ***information*** contained in this *Acceptable Use Policy*. Records demonstrating the completion of such training will be maintained and reported to the employee's manager. Security awareness will be made easily available for Commonwealth Agencies and Offices to provide to state employees.

6.1.2 Ongoing:

All Commonwealth Agencies and Offices must ensure that their ***personnel*** participate in regular ***information*** security awareness training, including mandatory participation in periodic social engineering (e.g., phishing) training exercises. ***Personnel*** must complete training on an annual basis. If changes have been made to the terms of the *Acceptable Use Policy*, ***personnel*** will acknowledge and agree to the ***Policy***. Records demonstrating the completion of such training will be maintained and reported to the Enterprise Security Office.

6.1.3. Job-Specific:

Commonwealth Agencies and Offices may have some job functions that require additional ***information*** security training and access agreements. The agency will provide additional training requirements as needed. Examples may include ***personnel*** who have access to systems that store ***confidential information*** such as Social Security information or job responsibilities such as developers and database administrators. The ***Commonwealth CISO,*** or his or her designee, will determine the job functions that require additional training and access agreements. ***Personnel*** must complete job-specific training on an annual basis.

6.1.4. Training Report:

A quarterly training report will be sent to the Enterprise Security Office to track overall completion rates. Individual training records are maintained in accordance with the statewide records retention schedule.

6.2. Acceptable Use of Information Assets

6.2.1. The Commonwealth's ***information assets*** further organizational goals and priorities. In using the Commonwealth's ***information assets***, Commonwealth Agencies and Offices will require their ***personnel*** to act in a professional and ethical manner and comply with their applicable Code of Conduct, relevant enterprise, and agency-level ***policies*** and/or applicable contractual obligations.

6.2.2. Use of Information Technology Resources

6.2.2.1. It is unacceptable for any person to use agency ***information*** technology resources:

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

6.2.2.1.2. For any political purpose

6.2.2.1.3. For any commercial purpose

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

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

6.2.2.1.6. To infringe any intellectual property rights

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

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

6.2.2.1.9. To intercept communications intended for other persons

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

6.2.2.1.11. To distribute chain letters

6.2.2.1.12. To access online gambling sites

6.2.2.1.13. To libel or otherwise defame any person

6.2.3. Email Use

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

6.2.3.1.1. Do not use email accounts for commercial purposes unrelated to Commonwealth business.

6.2.3.1.2. 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.

6.2.3.1.3. 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.

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

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

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

6.2.4. Use of Technology Assets

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

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

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

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

6.2.4.1.4. ***Users*** will not use personal devices to conduct Commonwealth business unless they have obtained prior approval from management. *(See IS.015 Asset Management Standard)*.

6.2.4.2. ***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.

6.2.4.3. 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.

6.2.5. Secure Transfer of Information

6.2.5.1. ***Confidential information*** will be securely exchanged through only authorized methods. ***Confidential Information*** will not be electronically transferred in an unencrypted or unprotected format. *(See IS.019 Cryptographic Management Standard)*.

6.2.6. Record Retention

6.2.6.1. ***Information*** storage and retention time frames will be limited to that required for legal, regulatory, and business purposes.

6.2.7. Secure Workspace

6.2.7.1. ***Personnel*** must keep their assigned workspace secure (e.g., lock ***confidential information*** in drawers, use cable locks if issued by Commonwealth).

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

6.2.8. Privacy and Monitoring

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

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

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

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

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

6.2.8.6. 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.

6.2.8.7. ***Users*** who 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***. *(See IS.015 Asset Management Standard)*.

6.3. Information Protection

6.3.1. Information classification - ***Personnel*** must adhere to the ***information*** classification system and ensure that appropriate measures are taken to protect ***information*** commensurate with its value to the Commonwealth.

6.3.2. The ***information*** classification system includes ***Restricted Information***, ***Confidential Information, General Information*** and ***Published Information***. *(See IS. Glossary of Terms for definitions and see Information Classification in IS.001 Information Security Governance Policy)*.

6.3.3. Information protection requirements - The confidentiality and integrity of ***information*** must be protected at rest, in use and in transit. ***Personnel*** must adhere to the following ***guidelines***.

6.3.3.1. Safeguards for Information at Rest:

6.3.3.1.1. Store all ***information*** on access-restricted and/or -controlled Shared Folders or Drives (e.g., SharePoint).

6.3.3.1.2. ***Encrypt*** or password-protect removable media that contains ***confidential information*** such as USB drives and mobile devices.

6.3.3.1.3. Dispose of ***confidential information*** only after confirming compliance with records retention laws.

6.3.3.2. Safeguards for Information in Use:

6.3.2.2.1. For access to systems that host ***confidential information***, ***personnel*** must request access using an approved access request process/tool and be positively authenticated (i.e., have an established ***user*** identity in Active Directory or another authentication source).

6.3.2.2.2. Use the minimum amount of ***confidential information*** (such as Social Security numbers) to the minimum necessary to support business operations (e.g., last four digits). Store the ***information*** in approved ***information*** repositories.

6.3.2.2.3. Do not store ***confidential information*** on laptops or desktops. ***Confidential information*** must be stored in Shared Folders, Shared Drives, or other secure Commonwealth systems.

6.3.2.3. Information in Transit

6.3.2.3.1. Use Commonwealth-issued ***encryption*** solutions to protect the integrity of ***confidential information*** that will be transmitted outside of the Commonwealth. This can be achieved by the following:

6.3.2.3.1.1. Use secure mail feature of email client by adding “[secure]” in the subject line to ***encrypt*** the email.

6.3.2.3.1.2. Password-protect files that contain ***confidential information*** *(See IS.019 Cryptographic Management Standard).*

6.3.2.3.1.3. Use the Commonwealth-approved secure transfer solution for larger transfers.

6.4. Access Management

6.4.2. Commonwealth Agencies and Offices must ensure that ***personnel*** are positively authenticated and authorized prior to receiving access to Commonwealth ***information*** resources.

6.4.3. Access to systems will be based on the ***user's*** role and must be limited to the minimum rights necessary to perform the ***user's*** job function.

6.4.4. Access to ***information assets*** must be controlled through a defined process, which includes a periodic review of ***information system*** privileges. *(See IS.014 Access Management Standard)*.

6.4.5. User Access to Information Systems

6.4.5.1. <u>Authorization</u>: ***Users*** must have an active ***user*** ID to access ***information assets*** on the Commonwealth family of networks.

6.4.5.2. <u>Authentication</u>: ***Information assets*** that access or store ***confidential information*** must authenticate a ***user's*** identity (e.g., password) prior to granting access.

6.4.5.3. <u>Access Requests</u>: ***Users*** must request access to technology infrastructure and/or ***applications*** required for job responsibilities using the Commonwealth-approved access request tools.

6.4.5.4. <u>Least Privilege</u>: ***Users*** must not be granted access to technology infrastructure and/or ***applications*** that are not required to perform the ***user's*** job responsibilities. ***Personnel*** will only be granted the minimum system resources and authorizations the ***user*** requires to perform the ***user's*** job functions. Managers are responsible for ensuring their direct reports have appropriate access to systems.

6.4.5.5. <u>Access Reviews</u>: Reviews of ***user's*** access to ***applications*** and/or technology infrastructure will be performed by managers at least annually to ensure access is appropriate to perform the ***user's*** job responsibilities.

6.4.5.6. <u>Segregation of Duties</u>: ***Users*** must not be granted access to ***information assets*** that would allow entitlements to perform job responsibilities that are not compatible with each other (e.g., having the ability to both request and approve a change).

6.4.6. Protect your password

6.4.6.1. Passwords provide a foundational security ***control*** to protect access to systems, technology infrastructure, ***applications***, and ***information***.

6.4.6.2. Agencies and Offices will adhere to the password requirements outlined in IS.*014 Access Management Standard*.

6.5. Network Access

6.5.1. Commonwealth network access is restricted to authorized ***users*** only.

6.5.2. ***Users*** must have a domain ***user*** identity to access the network.

6.5.3. Wireless Access

6.5.3.1. To improve mobility, connectivity and collaboration opportunities, the Commonwealth provides two wireless (Wi-Fi) networks, ‘secured’ and ‘public’, at certain office locations.

6.5.3.2. ***Users*** must be aware that not all internal ***applications*** will be available through the public Wi-Fi.

6.5.3.3. ***Personnel*** who wish to use wireless connections to conduct Commonwealth business may be required to connect to the secured Wi-Fi network.

6.5.4. Remote Access

6.5.4.1. ***Users*** who access the Commonwealth network remotely must be authenticated prior to establishing a network connection.

6.5.5. Physical Access

6.5.5.1. Commonwealth facilities and ***information assets*** must have appropriate physical access ***controls*** to protect them from unauthorized access.

6.5.5.2. ***Users*** must have a Commonwealth-issued badge and be prepared to show it if requested by building security.

6.5.5.3. Only authorized individuals are allowed into access-controlled areas. Visitors are allowed but must be escorted in controlled areas.

6.5.5.4. Circumventing established access ***control*** systems (e.g., propping doors open or tampering with turnstiles) is prohibited.

7. Control Mapping

Section	NIST SP800-53 R5	CIS 18 v8	NIST CSF
Policy Statements	PL-4	-	
	PS-6	-	

8. Related Documents

Document	Effective date
Code of Conduct (business unit specific)	
Cryptographic Management Standard	
Asset Management Standard	
Access Management Standard	

9. Document Change Control

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting
0.92	John Merto	01/02/2018	Corrections and formatting
0.95	Sean Vinck	5/7/2018	Corrections and formatting
0.96	Andrew Rudder	5/31/18	Corrections and formatting
0.97	Anthony O’Neill	05/31/2018	Corrections and formatting
1.0	Dennis McDermitt	6/1/2018	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; Corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	8/29/2022	NIST 800-53r5 update and Annual Review
1.4	Thomas McDermott	6/20/2023	Corrections, formatting, updating and Annual Review
1.4	Anthony O’Neill	6/21/2023	Final Review
1.5	Thomas McDermott	11/5/2024	Corrections, Formatting and Annual Review
1.5	Anthony O’Neill	11/5/2024	Final Review
1.6	Thomas McDermott	2/6/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	2/25/2025	Corrections and Formatting
1.6	Anthony O’Neill	3/4/2025	Final Review