Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Enterprise Asset Management Policy

Document Name: Asset Management Policy	Effective Date: 1/1/2025
Document ID: IS.004	Last Revised Date: 12/23/2024

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*** technology environment. This ***policy*** reinforces the Commonwealth's commitment to an effective ***asset*** management program. This document outlines ***asset*** management requirements to protect information and reduce ***risks*** posed by improper management of IT ***assets*** within 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 voluntarily 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. Additional ***information*** regarding this ***policy*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/***policies.*** Definitions of terms in bold may be found in the ***IS Glossary*** 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. ***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. All ***exceptions*** will be for a limited time and will be narrow in scope.

6. Requirements for Asset Management

6.1. ***Assets*** may be tangible (e.g., computers, mobiles, network equipment and media) or intangible (***information***-related – e.g., ***information***, ***data***, ***software***, and services).

6.2. Commonwealth Agencies and Offices will identify, inventory and classify all ***assets***, both tangible and intangible, on a continuous basis.

6.3. Asset Inventories:

6.3.1. ***Asset*** inventories must include all ***information*** necessary to effectively manage the ***asset*** throughout its lifecycle, from creation through disposal.

6.3.2. ***Information*** necessary for the effective management of identified ***assets*** must be collected and documented. ***Information*** on its sensitivity, owner, handling requirements, retention limits, and disposal requirements must be recorded in the inventory.

6.3.3. The ***asset*** inventory must be reviewed and updated on a continuous basis, but not less than annually.

6.4. Asset Ownership:

6.4.1. An ***information owner*** will be identified for all ***assets***. The ***Information Owner*** will remain responsible for the management and security of the ***information asset,*** including ***asset*** classification, access restrictions, and ***risk*** mitigation of end-of-life/end-of-support ***assets***.

6.5. Asset Identification:

6.5.1. ***Data*** and ***information*** processing and storage must be segmented based on the sensitivity of ***data***.

6.5.2. An automated tool must be used to identify where ***data*** is stored, processed, and transmitted through enterprise ***information assets***. The ***information*** generated by the automated tool must be used to update the ***data*** and ***information*** inventory.

6.5.3. Unauthorized ***assets*** will be detected using automated tools and must be removed from the network, denied remote access, and/or quarantined.

6.5.4. The flow of ***data*** and ***information*** through the Enterprise's processes and systems must be documented and documentation reviewed not less than annually.

6.6. Use of Assets:

6.6.1. Only currently supported and approved ***software*** is authorized for use on any Commonwealth system or network. Commonwealth Agencies and Offices must submit an ***exception*** request as detailed above, to receive approval for the use of unsupported ***software***.

6.6.2. Maintenance of all ***assets*** must be performed in accordance with the manufacturer's/supplier's recommendations and tested periodically.

6.6.3. Commonwealth Agencies and Offices will implement ***endpoint*** security ***controls***, including ***endpoint*** detection and response (EDR) solutions to protect ***assets*** against anomalous activity and malicious ***software***, including viruses and ***malware.***

6.6.4. Implement technical ***controls*** to restrict the installation of unauthorized ***software*** on Commonwealth-owned or managed ***endpoints***.

6.6.5. Commonwealth Agencies and Offices will Configure antivirus and/or EDR solutions so that they cannot be circumvented, disabled, or removed from an ***endpoint*** by an end ***user***.

6.6.6. Commonwealth Agencies and Offices will implement ***controls*** to protect ***endpoints*** from viruses and ***malware*** that can be introduced via removable media. At a minimum, the ***controls*** will include:

6.6.6.1. Auto scan removable media for virus and ***malware*** prior to use.

6.6.6.2. Disable functionality that allows auto-run upon insertion of removable media.

6.6.6.3. Force ***encryption*** on removable media prior to allowing ***information*** transfer to and from the media.

6.6.6.4. Prevent the installation of unauthorized ***software*** on Commonwealth-owned or managed ***endpoints*** from removable media.

6.6.7. Equipment must only be taken off-site for valid business reasons and with authorization from the ***information owner***. Equipment taken off-site must be physically protected by the individual taking the equipment off-site.

6.6.8. Commonwealth Agencies and Offices must ensure that Commonwealth-issued or managed devices, (e.g., laptops, cell phones and/or tablets), do not leave the United States.

6.6.9. Organizationally owned equipment must be returned within ten (10) business days upon termination of ***personnel*** and expiration of external business relationships.

6.6.10. All ***information*** must be removed or securely overwritten prior to the disposal and reuse of equipment.

6.7. Asset Classification:

6.7.1. The ***information asset*** owners are responsible for establishing ***asset*** classification.

6.7.2. The classification of all ***assets***, including the sensitivity level of all ***information assets***, must be established to apply the appropriate security measures.

6.7.3. The classification or sensitivity level of all ***assets*** must be commensurate with their value to the organization and in accordance with organizational, legal, and regulatory requirements.

6.7.4. ***Information systems*** must be classified by the ***information owner*** based on the system's most critical component.

6.7.5. Procedures for the handling and labeling of ***data*** and ***information*** must be defined, maintained, and follow legal and regulatory obligations.

6.7.6. The use of ***encryption*** must be implemented to protect ***data*** at rest and in transit commensurate with its classification level.

6.7.7. Automated technologies approved and managed by EOTSS will be utilized for ***data*** monitoring.

6.7.8. ***Information*** will be retained in accordance with legal and regulatory obligations and in alignment with the Massachusetts Statewide Records Retention Schedule.

6.7.9. ***Asset*** classification must be reviewed and updated not less than annually.

7. Mobile Device Management

7.1. Commonwealth Agencies and Offices will create and actively maintain an inventory of ***mobile devices*** authorized to connect to the Commonwealth's IT environment. The inventory must be reviewed at least annually and include ownership ***information*** and device specifications (e.g., manufacturer, model, OS).

7.2. All ***mobile devices*** that directly connect to the Commonwealth family of networks or that have direct access to the Commonwealth's ***information assets***, must connect via VPN, must be secured with a password that meets or exceeds the access control requirements, must adhere to the ***encryption*** requirements issued by EOTSS.

7.3. Commonwealth Agencies and Offices must ensure ***mobile device users*** are aware of the ***risks*** involved with mobile computing and the types of ***information*** that can and cannot be stored on such devices, through regular security awareness training.

7.4. ***Users*** are prohibited from making modifications of any kind of Commonwealth owned or installed hardware and/or ***software*** on the mobile device.

7.5. Mobile devices, regardless of ownership, housing any form of Commonwealth ***information*** will be securely decommissioned, when no longer needed for business or legal reasons.

7.6. The Commonwealth will implement a mobile device management (MDM) solution, approved, and maintained by EOTSS, to manage mobile devices in its environment, that includes the following ***controls***:

7.6.1. Prevent unauthorized disclosure of ***information*** on mobile devices (e.g., mobile phones and tablets).

7.6.2. Provide the highest coverage of mobile devices and operating systems

7.6.3. Have the ability to remotely update firmware and ***applications*** on mobile devices.

7.6.4. Include ***information*** and device ***encryption***, device monitoring, logging and tracking, ***information*** segmentation, password/PIN management, remote wipe, backup and restore.

7.7. ***Users*** who voluntarily choose to use their personal mobile device to directly access Commonwealth ***information***, and/or to conduct any form of Commonwealth business must acknowledge in writing that they understand and accept the following:

7.7.1. ***Users*** must obtain prior authorization from their agency to use their personal mobile device to conduct any form of Commonwealth business.

7.7.2. ***Personnel*** should have no expectation of privacy with respect to any Commonwealth owned, or managed device used to conduct any form of Commonwealth business. Network administrators routinely monitor network traffic.

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

7.7.4. Any Commonwealth owned, or managed device used to conduct any form of Commonwealth business is subject to monitoring, and review, and may be logged, recorded and/or investigated. The Commonwealth retains the authority to review and retrieve ***information*** from, and remotely wipe any Commonwealth owned, or managed device.

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

7.7.6. ***Personnel*** must understand and accept the ***risks*** associated with using a mobile device that is owned or managed by the Commonwealth, including

inclusion in the mobile device inventory, installation of an MDM solution, and enforcement of password policies.

8. Roles and Responsibilities:

Role	Responsibility
Commonwealth Chief Information Security Officer (CISO)/Chief Risk Officer (CRO)	The person responsible to ensure compliance with this policy across all Commonwealth Agencies and Offices. The CISO leads the ERM Office and is responsible to align security initiatives with enterprise programs and business objectives. The CISO ensures that all of the Commonwealth's IT assets, communication systems, data and technologies 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.
EOTSS Security Operations Center (SOC)	The office within EOTSS responsible for monitoring and analyzing the state's security posture, and for detecting, analyzing and responding to cybersecurity incidents. The SOC coordinates with municipal, state, and federal agencies, as well as other stakeholders, in the event of a cybersecurity incident. The SOC is also responsible for communicating any high or critical situations to leadership, and for sharing information and resources as needed, to mitigate the effect of an incident.
Chief Technology Officer (CTO)	The person responsible for the management, implementation, security and internal operations of the entire information technology department. 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.
General Counsel's Office (GC)	The GC's office within EOTSS is responsible for providing advice to both EOTSS and other Commonwealth Agencies and Offices regarding asset management. The GC's office identifies legal issues based on changes in statutes, regulations, contracts and judicial

	opinions. Provides guidance and support to business units and other Commonwealth agencies regarding privacy, and asset management issues.
Data/Information Asset Owner	Responsible for the management and security of data/information assets. Responsible for assigning classification/sensitivity levels to assets and ensuring protection is commensurate with the value of the asset to the Agency or Office.
Commonwealth Agencies and Offices	Commonwealth Agencies and Offices are responsible to adhere to this policy and to comply 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.

9. Control Mapping

Section	NIST 800-53	CIS 18	NIST CSF
Information Asset Management/Data Management	AC-3, AC-4, AC-6, AC-13, CM-8, IA-3, IA-7, MA-2, MP-3, MP-5, MP-6, RA-3, RA-9, PM-5, PM-7, SC-13	1.1 – 1.5, 2.1 – 2.7, 3.1 – 3.14	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08
Information Asset Classification/Data Classification	AC-16, IA-3, IA-7, MP-3, MP-6, PM-7, SC-13	1.1 – 1.5, 2.1 – 2.7, 3.1 – 3.14	ID.AM-05
Data and Information Asset Labeling and Handling	IA-3, IA-7, MP-3, MP-6, PM-7, SC-13	1.1 – 1.5, 2.1 – 2.7, 3.1 – 3.14	ID.AM-05
Mobile Device Management	AC-19, IA-3, IA-7, MP-3, MP-6, PM-7, SC-13	1.1, 1.2, 1.3, 1.4, 2.1, 2.2, 2.3, 1.5,	ID.AM-01, ID.AM-02, ID.AM-08

10. Document Change Control

Version No.	Revised By	Effective Date	Description of Revisions
1.0	Vendor	6/10/2024	Initial 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