Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Enterprise Access Management Policy

Document Name: Access Management Policy	Effective Date: 1/1/2025
Document ID: IS.003	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 grant, manage, and revoke *user* and system accounts. This ***policy*** reinforces the Commonwealth's commitment to an effective account management program. This document outlines account management requirements to safeguard *assets* and reduce *risks* posed by improper management of account identifiers and authenticators 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

6.1. Access Management

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

6.1.2. 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.

6.1.3. Access to ***information assets*** must be controlled through a defined ***process***, which includes a periodic review of ***information system*** privileges.

6.1.4. Commonwealth Agencies and Offices will maintain an inventory of all accounts, including ***user*** accounts, administrator accounts, service accounts, system accounts and Firecall accounts. This inventory will be reviewed annually.

6.1.5. Authorization: ***Users*** must have an active ***user*** ID to access ***information assets*** on the Commonwealth family of networks.

6.1.6. Authentication: ***Information assets*** that access or store ***restricted***, ***confidential,*** and/or ***general information*** must authenticate a ***user's*** identity

(e.g., password) prior to granting access. Passwords provide a foundational security ***control*** to protect access to systems, technology infrastructure, ***applications***, and ***information.***

6.1.7. ***Users*** must adhere to all ***agency*** password requirements and are responsible for protecting their passwords.

6.1.8. Access requests: ***Users*** must request access to technology infrastructure and/or ***applications*** required for job responsibilities using the Commonwealth-approved access request tools.

6.1.9. Least privilege: ***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.

6.1.10. Annual review: Managers will review the ***user*** access of their direct reports to ***applications*** and/or technology infrastructure, on an annual basis, to ensure each ***user's*** access is appropriate to perform the ***user's*** job responsibilities.

6.1.11. Segregation of duties: ***Users*** must not be granted access to ***information assets*** that would allow system permissions to perform job responsibilities that are not compatible with each other (e.g., having the ability to both request and approve a change).

6.1.12. ***Multi-Factor Authentication (MFA)*** is required for all externally exposed ***applications***, remote network access, and administrative access.

6.1.13. Network Access: The Commonwealth network is restricted to authorized ***users*** only. ***Users*** must have a domain ***user*** identity to access the network.

6.1.14. Wireless Access: To improve mobility, connectivity and collaboration opportunities, the Commonwealth provides two wireless (Wi-Fi) networks; 'secured' and 'public', at certain office locations.

6.1.15. ***Users*** must be aware that not all internal ***applications*** will be available through public Wi-Fi. ***Personnel*** who wish to use wireless connections to conduct Commonwealth business may be required to connect to the secured Wi-Fi network.

6.1.16. Remote Access: ***Users*** who access the Commonwealth network remotely must be authenticated through the use of ***Multi-Factor Authentication (MFA)*** prior to establishing a network connection.

6.1.17. Commonwealth Agencies and Offices must establish a documented ***procedure*** to grant access to the Commonwealth's ***information assets*** during an emergency in accordance with the Enterprise Incident Management Policy.

6.2. Granting and Modifying Access

6.2.1. Commonwealth Agencies and Offices must establish a documented ***procedure*** to grant access to the Commonwealth's ***information assets*** for new hires.

6.2.2. Commonwealth Agencies and Offices must establish a documented ***procedure*** to grant and/or revoke access in the ***event*** of a role change.

6.2.3. All access requests for both new hires and role changes must be recorded (paper or tool-based) and include both a business justification and management approval.

6.2.4. Permissions are granted based on the principle of least privilege. ***Users*** will only receive the permissions needed to perform their individual job responsibilities.

6.2.5. Remote, wireless and mobile access will only be permitted for employees and ***contractors*** with a valid authorization and will be provisioned by ***security administrators*** in alignment with approved configurations.

6.2.6. The creation and/or existence of non-built-in shared accounts is prohibited unless an ***exception*** is obtained as detailed above. All ***exception***-based shared account access will be time-boxed.

6.2.7. Commonwealth Agencies and Offices will establish and maintain dedicated ***administrator accounts*** that are separate from accounts used to perform daily tasks. These accounts are only used to perform administrative actions.

6.3. Revoking Access

6.3.1. Commonwealth Agencies and Offices will establish documented ***procedures*** for revoking access to enterprise ***assets*** for terminated ***users*** that preserves audit trails.

6.3.2. Account managers and ***security administrators*** must be notified when an account is no longer required, whether that is due to termination, role change, or other significant changes to a ***user's*** employment status or role.

6.3.3. Commonwealth Agencies and Offices will disable dormant accounts not less than annually.

6.3.4. Any privileged access no longer required by a ***user*** to fulfill an individual's job role will be removed.

6.3.5. ***Security administrators*** in consultation with the Enterprise Risk Management Office (or ***agency's Information Security Team***) may temporarily suspend or restrict a ***user's*** level of access to the network if the account is suspected of privilege abuse or violation of the Acceptable Use Policy.

6.4. Password Management

6.4.1. Commonwealth Agencies and Offices will require the use of unique passwords, password complexity, password expiration, and password character order to protect the Commonwealth's ***information*** resources.

6.4.2. Passwords must expire or change, as follows:

6.4.2.1. Require change of initial (or temporary) password upon first-time login/use. Initial passwords must be unique for each ***user*** and received in a secure manner.

6.4.2.2. Passwords/PINs must be changed immediately if a compromise is suspected.

6.4.2.3. ***User*** accounts must be changed at least once every 180 days and administrator accounts must be changed at least once every 90 days.

6.4.2.4. Enforce a minimum password age of at least one (1) day.

6.4.2.5. Service account passwords must be changed every 180 days.

6.4.2.6. The use and management of one-time use or temporary passwords will be managed in a manner that complies with this ***policy.***

6.4.2.7. Commonwealth Agencies and Offices must ensure that ***security administrators*** positively verify the identity of a ***user*** prior to a password reset.

6.4.2.8. Only the individual to whom the ***user*** ID is assigned may request a password reset.

6.4.2.9. Password resets must not be performed prior to verification of the requestor's identity.

6.4.2.10. Both the ***user*** ID and password must be authenticated in their entirety. If authentication fails, the system error message must not indicate which component of the ***user's*** input (***user*** ID or password) is incorrect (e.g., "incorrect login," or "incorrect password").

6.4.2.11. All passwords must be stored in a secure manner in order to protect the Commonwealth's ***information*** resources.

6.5. Information Systems

6.5.1. Commonwealth Agencies and Offices will configure ***information systems*** with appropriate authentication ***controls*** designed to prevent unauthorized disclosure, modification, or access to ***information***.

6.5.2. Network devices and systems must be configured with appropriate ***access controls*** to prevent unauthorized modification or access to ***information assets*** and internal and external networked devices.

6.5.3. Other than use of publicly available websites and systems, no ***user*** actions may be performed within systems without identification and authentication of the ***user***.

6.5.4. Workstations left unattended for extended periods of time must be locked or logged off.

7. Roles and Responsibilities

Role	Responsibility
Enterprise Risk Management (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 ensure compliance with applicable laws, rules and regulations. ERM works 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.
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 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.
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.
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.
Administrators	Responsible for implementing the controls, configurations, and procedures listed in this policy.

8. Control Mapping

Section	NIST 800-53R5	CIS 18 v8	NIST CSF
6.1	AC-1	5.6	
	AC-2	-	
6.2	AC-2(1)	6.6	
6.3	AC-2	5.1	
	-	5.5	
6.4	AC-2(4)	6.1	
	AC-2(11)	6.2	
6.5	AC-2(7)	5.4	
6.6	AC-2(9)	-	
6.7	AC-3(3)	6.8	
6.8	AC-2(3)	5.3	
	-	6.2	
6.9	AC-3	5.2	
	AC-3(2)	6.3	
	-	6.4	
	-	6.5	

9. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/6/2024	Initial Access Management Policy Draft
1.1	Thomas E. McDermott	8/9/2024	Revisions, Corrections, Formatting
1.2	Miklos Lavicska	9/25/2024	Corrections, Formatting
1.3	Thomas E. McDermott	12/23/2024	Revisions, Corrections, Formatting
1.4	Anthony J. O'Neill	1/1/2025	Final Review