



Access Management Policy

Effective Date:
June 10, 2026

Category:
Security

Scheduled Review:
June 2027

1. Authority

[Executive Order 2016-06, Enterprise Information Technology Governance](#)

2. Document Control

This procedure replaces, in its entirety, the Access Management Policy, dated March 11, 2025.

3. Purpose

This policy establishes the requirements for the management, control, and monitoring of privileged access to Commonwealth IT Resources.

4. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

5. Policy

For definitions of terms found within this document, refer to the [IT Policy Glossary](#).

5.1 Privileged User Account Types

Privileged User account types include:

- Administrative Accounts
- Service or Operational Accounts (with elevated privileges)
- System accounts

All Privileged Accounts shall be properly secured and monitored in accordance with this policy and *Management Directive 245.18 Amended, IT Administrator Acceptable Use, Auditing and Monitoring*.

5.2 General Privileged Account Requirements

The following requirements apply to all Privileged Accounts:

- Access requires explicit approval from the agency Information Security Officer (ISO).
- Privileged Users shall complete required security awareness and IT administrator acceptable use training prior to access.
- Accounts shall comply with the *User Authentication Standard*.
- Accounts shall uniquely identify and authenticate a specific user, process, or system.
- Privileged Account passwords are prohibited from being shared.
- Access shall follow the principle of Least Privilege.
- Access shall be assigned using Role-Based Access Control (RBAC).
- Agencies shall maintain a current inventory of all Privileged Accounts.
- Privileged Accounts shall be monitored and audited.
- Privileged access shall be reviewed at least every six months and adjusted as necessary.
- Agencies shall conduct semi-annual reviews or scans to identify undocumented or excessive privileged access.

5.3 Service or Operational Accounts

Service and Operational Accounts with elevated privileges shall be documented and managed in accordance with the *User Authentication Standard*.

5.4 System Accounts

Built-in or default system accounts shall be used only when no alternative exists.

Where possible, default accounts shall be disabled; otherwise, they shall be renamed.

Default credentials shall be changed and managed in accordance with the *User Authentication Standard*.

5.5 Reporting of Non-Compliant Systems and Applications

Non-compliant or legacy systems shall be documented via an IT Policy Exception as detailed in section 7 below. The exception shall include the nature of non-compliance, data sensitivity, compensating controls, and remediation or replacement plans.

6. Contact

Questions or comments may be directed via email to [OA, IT Policy](#).

7. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

8. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document
Revision	03/11/2025	Added Document Control Section Added requirement for security awareness and IT administrator acceptable use training Alignment with <i>Management Directive 245.18</i> (ISO approves privileged accounts) Alignment with NIST 800-53 Clarified that shared Privileged Accounts are prohibited Clarified when Privileged Accounts should be disabled or removed Added requirement to review inactive or unused accounts Added reference to <i>Security Logging and Event Monitoring Standard</i>.
Revision	06/10/2026	Reworded to make more concise and remove redundancy Updating the reporting of non-compliant systems to be via policy exception Moved the details around the naming of break-glass accounts to a non-public document (<i>User Authentication Standard</i>) Misc. clarifications