Information Technology Policy

Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication

Number ITP-SEC007	**Effective Date** March 1, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** May 2025

1. Purpose

This Information Technology Policy (ITP) establishes minimum standards for the implementation and administration of users, Systems, networks, devices, application account IDs, passwords, sessions, and requirements around Multi-Factor Authentication (MFA).

The use of IDs, passwords, sessions, and MFA provides for Authenticated and Authorized access to:

- The enterprise Local Area Network (LAN)/Wide Area Network (WAN)
- Enterprise applications (e.g., Email servers and client applications, Virtual Private Network (VPN), file transfer systems, databases)
- Agency applications
- Systems (servers, personal computers, routers, etc.)
- Peripheral equipment (printers, copiers, multi-function devices, etc.)

2. Scope

This ITP 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").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Policy

Within thirty days of the date of issuance of any revision to this ITP and/or *OPD-SEC007a, Configurations for IDs, Passwords, and Multi-Factor Authentication*, agencies shall implement the specified access controls to standardize account ID, password, and session controls in all computer Systems and application environments.

Systems and applications that do not comply with this policy will have 12 months from the date of the last policy update to ensure compliance with this policy. Those Systems or applications that are not currently in compliance will require reporting, which includes providing any scheduled update plans for the System or application as specified below in *Section 4, Reporting of Non-Compliant Systems and Applications.* Agencies who have a System or application that is unable to meet this requirement must obtain an IT policy waiver following the guidance below in *Section 9, Exemption from this Policy.*

New applications, whether Commercial-off-the-Shelf (COTS) or wholly custom-built, that cannot employ the enterprise directories and cannot adhere to the account ID and password standards listed in *OPD-SEC007a, Configurations for IDs, Passwords, and Multi-Factor Authentication*, must obtain a waiver to this ITP prior to going live (*Section 9, Exemption from this Policy*) and must report these applications per *Section 4, Reporting of Non-Compliant Systems and Applications.*

All computers or other devices, including hosted applications, permanently or intermittently connected to Commonwealth networks, must have minimum access controls (account ID and password) unique to the owner of the account.

MFA must be implemented for users requiring direct access to internal Systems hosting or processing sensitive data from the Internet.

Details of the Commonwealth account ID and password policies are contained in *OPD-SEC007A, Configurations for IDs, Passwords, and Multi-Factor Authentication*.

3.1 Inactivity:

Accounts that have not been utilized in 18 months or one that lacks any role or related attribute that would be used to authorize its use to access an IT System shall be disabled. In the case of an Active Directory (AD) account, the AD userAccountControl attribute shall be set to "Disabled."

Session Inactivity when there has been user activity by a user logged on to the Commonwealth network for CWOPA accounts shall not exceed fifteen (15) minutes per session. After this period of Session Inactivity, the user will be required to reauthenticate to re-establish access to the System.

Applications, with the exception of Outlook and Microsoft 365 applications, shall logout users after 20 minutes of inactivity within that application. After this period of application inactivity, the user will be required to reauthenticate to re-establish access to the application.

Enterprise Directory Sessions:

	CWOPA	Managed Users	SRPROD
Account Lockout	After 5 failed attempts	After 5 failed attempts	After 5 failed attempts
Session Inactivity	Lock PC after 15 min	N/A	N/A
Application Inactivity	Logout after 20 min	Logout after 20 min	Logout after 20 min
Maximum Session Lifetime	Logout after 24 hrs	Logout after 24 hrs	Logout after 24 hrs

Privileged (Local & System Administrators) Account Sessions:

Account Lockout	After 5 failed attempts
Application Inactivity	Logout after 10 hrs
Maximum Session Lifetime	Logout after 24 hrs

The above specifications for sessions apply to Non-Enterprise Directories (e.g. directories, databases or database tables, etc.) or devices, such as hand held or mobile devices, mainframes, and network devices, that are used to provide Authentication and security access to Commonwealth System resources and applications where the use of Enterprise Directories is not technically possible. Note that this is not an endorsement of the use of Non-Enterprise Directories but only an acknowledgment that they exist. Also, use of Non-Enterprise Directories may require a waiver to one or more other ITPs as dictated by the specific application or System.

4. Reporting of Non-Compliant Systems and Applications

Compliance with the requirements of this policy shall be reviewed as part of the security assessment required by *ITP-SEC023, Technical Security Assessments Policy*. In instances where an independent third party is completing the security assessment and non-compliance is identified, it shall be reported to the agency Information Security Officer (ISO) and the Commonwealth Chief Information Security Officer (CISO). The report shall include user ID and password policy details, the type of data stored on the System or accessed by the application, all compensating controls, and any plans for the revision or replacement of the System or application to bring it into compliance.

5. Responsibilities

5.1 Agencies shall:

- Comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office for Information Technology shall:

- Comply with the requirements as outlined in this ITP.

5.3 Third-party vendors, licensors, contractors, or suppliers shall:

- Utilize the Commonwealth's enterprise directories and password policies.
- Implement MFA for users requiring direct access to a System from outside the Commonwealth network. Where possible, the Commonwealth's MFA solution shall be utilized.
- For Systems containing Class "C" or Closed records, per *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Electronic Data*, MFA shall be implemented.

6. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx
- *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*
- *Management Directive 205.34,* Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 245.18, IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures*
- OPD-SEC007A - *Configurations for IDs, Passwords, and Multi-Factor Authentication* (Commonwealth Access Only)
- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC019, Policy and Procedures for Protecting Electronic Data*
- *ITP-SEC023, Technical Security Assessments Policy*
- *ITP-SEC024, IT Security Incident Reporting Policy*
- *ITP-SEC031, Encryption Standards*
- *ITP-SEC038, Commonwealth Data Center Privileged User Identification and Access Management Policy*
- *ITP-SEC039, Keystone Login and Identity Proofing*
- *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Electronic Data*
- *NIST Special Publication SP 800-118, Guide to Enterprise Password Management* (Retired Draft)
- *NIST Special Publication SP 800-63-3, Digital Identity Guidelines*
- *NIST Special Publication SP 800-63A, Digital Identity Guidelines: Enrollment & Identity Proofing*
- *NIST Special Publication SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management*
- *NIST Special Publication SP 800-63C, Digital Identity Guidelines: Federation and Assertions*
- *NIST Special Publication SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations*
- *NIST Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. Publication Version Control

It is the Authorized Users' responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

9. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original		Base Document	N/A
Revision	05/17/2010	Add language to address legacy applications	N/A
Revision	04/02/2014	ITP Reformat Merged RFD-SEC007A, RFD-SEC007B, RFD-SEC007C, BPD-SEC007D into ITP	N/A
Revision	05/05/2015	Rewrite of Purpose section Added Systems Added Peripheral equipment Expanded and clarified Scope section Expanded and clarified Objective section Added Definitions section Expanded: Section 5 General Policy Section 6 Detailed Policy Revised language in CoPA Systems Log-In/Log-Off Process Policy Added Reporting of non-Compliant… as its own sectionExpanded Related ITPs/Other References	N/A
Revision	03/09/2016	Added "Multi-factor Authentication" to ITP Title Added sub section 6.9 detailing multi-factor authentication requirements Added multi-factor authentication to various areas throughout ITP Added Risk-based authentication (RBA) definition	N/A
Revision	12/15/2016	Added GUID and Permanence definitions Added ITP-SEC019 reference	N/A
Revision	12/07/2017	Added definitions/language regarding inactive accounts and purging Revised language throughout for clarity Created OPD-SEC007A	N/A
Revision	10/10/2019	Reviewed OPD-SEC007A revised	N/A
Revision	9/22/2020	Reviewed OPD-SEC007A revised	N/A
Revision	09/21/2021	• Updated Title • Definition Section updated • Added Section 5.1 Sessions • Added third party vendors to Scope and Responsibilities sections.	N/A

Version	Date	Purpose of Revision	Redline Link
		- Updated References/added links OPD-SEC007a revised	
Revision	05/06/2022	Updated requirements for third party vendors in Responsibilities section.	N/A
Revision	07/12/2022	Reviewed OPD-SEC007A revised	N/A
Revision	10/18/2022	OPD-SEC007A revised Updated Scope – language makes inclusive of any entity connecting to the Commonwealth Network Added ITP-SEC038 to References section	N/A
Revision	05/02/2024	Annual Review OPD-SEC007A updated Updated Purpose to remove specific product names Removed Objectives Definitions section removed from policy. Definitions added OA Glossary and linked throughout policy. Timeline added around compliance for systems and applications with policy. Updated policy references in policy were required (ITP-SEC023 policy title, added references to ITP-INF015 and added reference to ITP-SEC039). General policy wording updates for consistency, intent not changed. Clarified Section 4. Reporting of Non-Compliant Systems	Revised IT Policy Redline <05/02/2024>