pennsylvania
OFFICE OF ADMINISTRATION

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
October 2023

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) (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., Exchange, Virtual Private Network (VPN) Outlook, Exchange, FTP 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. Definitions

Account Lockout: The disabling or suspension of an account ID, generally as a result of a number of failed attempts to authenticate with that account ID.

Application Inactivity: The length of time an application is accessed (i.e., the account ID is logged in) without any interaction with the user.

Disable: An account may be Disabled either by setting the Active Directory (AD) userAccountControl attribute (set the 0x200 bit to 1) or by moving the account to a dead storage area where it will not be used for Authentication purposes.

Globally Unique Identifier (GUID): An alpha-numeric code that uniquely identifies a person. Two John Smiths could, for instance, both have the same user ID, but they would have different GUIDs. User access to IT resources should be based on the GUID rather than the user ID as it uniquely identifies the person. Note: Active Directory assigns a GUID to each *account*, this is not necessarily the same as assigning a GUID to a *person*.

Inactive Account: An Inactive Account shall be any account that hasn't been used in 18 months or one which lacks any role or related attribute that would be used to authorize its use to access an Information Technology System; or any account where the AD userAccountControl attribute is set to "Disabled".

Information Technology Systems or Systems: Where referenced in this ITP, Information Technology Systems or Systems include computer applications, servers, laptops, databases, routers, switches, wireless devices, mobile devices and other computer related hardware and software.

Maximum Session Lifetime: The maximum time a System, device, or application may be accessed by a user, regardless of the user's activity, before the user must re-authenticate to the System, device, or application.

Non-Enterprise Directories: All other Commonwealth user directory stores that are not Enterprise Directories.

Privileged (Local Administrator) Accounts: Local Administrator Accounts referenced in this section are defined as accounts having privileges beyond standard user-level access privileges, for accessing servers, workstations (PCs, laptops, etc.), printers, routers, network switches, firewalls, wireless access points, databases, applications, and other Information Technology Systems. Local Administrator accounts are typically generated, maintained, monitored and managed on an individual machine-level, system-level, application-level or database-level basis.

Privileged (System Administrator) Accounts: Privileged or Administrator Accounts generally have elevated or full access rights to Systems, devices, and applications. This allows them to change system or device configurations and access data with full read-write privileges. They can create, delete, or modify user accounts and install software. The level of security protecting such accounts needs to be higher than a normal user account.

Session Inactivity: The length of time a System or device is accessed (i.e., the account ID is logged in) without any interaction with the user.

4. Objective

The objective of this ITP is to:

- Provide security requirements for accessing computer applications, Systems and data with User IDs, passwords, sessions, and MFA techniques.
- Provide a level of standardization and uniformity throughout agencies for User ID/password, sessions, and MFA implementation and management.
- Ensure compliance with federal and other external requirements where possible.

5. Policy

Within thirty days of the date of issuance of this revised ITP, agencies shall implement the specified access controls, as enumerated in this ITP, to standardize account ID, password, and session controls in all computer Systems and application environments. MFA should be implemented for users requiring direct access to internal Systems hosting or processing sensitive data from the Internet.

Recognizing the existence of legacy and other pre-existing Systems and applications, which are not in compliance with this policy and for which it may not be feasible to bring into compliance with this policy, such Systems and processes will be "grandfathered" in upon reporting and providing any scheduled update plans for the System or application as specified below in *§6.0 Reporting of non-Compliant Systems and Applications.*

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*, as listed below, will need to obtain a waiver to this ITP prior to going live (*§11.0 Exemption from this Policy*) and will need to report these applications per *§6.0 Reporting of non-Compliant Systems and Applications.*

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

Details of the Commonwealth account ID and password policies are contained in OPD-SEC007A, *Configurations for IDs, Passwords, and Multi-Factor Authentication*, available upon request from the Enterprise Information Security Office.

5.1 Sessions:

Session Inactivity occurs when there has been no activity on a System or application after a designated amount of time after a user has logged into the System or application. When Session Inactivity has occurred, the System or application will be locked or logged out of (depending on the requirements) and the user will be required to provide a user ID and password to re-establish access to the System or application. The period of Session Inactivity to the Commonwealth network shall not exceed fifteen (15) minutes per session. An exception to this policy shall be made in those cases where the immediate area surrounding a System is physically secured via

cipher locks, secured-room badge readers, or similar technology.

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.

6. Reporting of Non-Compliant Systems and Applications

In the case of non-compliant Systems or legacy applications, the non-compliance shall be reported to the agency security officer and the Chief Information Security Officer for the Commonwealth of Pennsylvania (CISO) as part of the agency's security assessment (*ITP-SEC023 – Information Technology Security Assessment and Testing Policy*). The report will include details as to the user ID and password policies, the type of data stored on the System or accessed by the application, any compensating controls, and any plans for the revision or replacement of the System or application.

7. Responsibilities

7.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

7.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

7.3 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" records or closed records (per ITP-SEC019), MFA shall be implemented.

8. 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* (Authorized Users Only)
- ITP-ACC001 – *Information Technology Digital Accessibility Policy*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*
- ITP-SEC031 – *Encryption Standards*
- ITP-SEC038 – *Commonwealth Data Center Privileged User Identification and Access Management Policy*
- 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*

9. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

10. Publication Version Control

It is the Authorized User's 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.

11. 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 section Expanded 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

Version	Date	Purpose of Revision	Redline Link
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. • Updated References/added links OPD-SEC007a revised	N/A
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	Revised IT Policy Redline <10/18/2022>