pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

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

ITP Number ITP-SEC007	**Effective Date** March 1, 2006
Category Security	**Supersedes**
Contact RA-ITCentral@pa.gov	**Scheduled Review** December 2018

1. Purpose

Establishes minimum standards for the implementation and administration of user, system, network, device, application account IDs, passwords, and requirements around multi-factor authentication.

Generally, the use of IDs, passwords and multi-factor authentication 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 Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Objective

The objective of this ITP is to:

- Provide security requirements for accessing computer applications, systems and data with UserIDs, passwords, and multi-factor authentication techniques
- Provide a level of standardization and uniformity throughout Commonwealth of PA (COPA) agencies for UserID/Password, and multi-factor authentication implementation and management
- Satisfy federal compliance requirements and other external requirements where possible.

4. 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.

Application Timeout: Maximum length of application inactivity after which the user's access is terminated or the application is shut down.

Authentication: The process of establishing confidence in the validity of a claimant's presented identifier, usually as a prerequisite for granting access to resources in an information system.

Authentication Method: The type of authentication being used to validate a claimant. These are categorized as:

- Something you know (e.g. PIN, password, shared information)
- Something you possess (e.g. token, smart card, digital certificate)
- Something you are (biometrics – e.g. fingerprint, voice, iris, face).

Authorization: The process of verifying that an authenticated user is permitted to have access to a system or application based on the user's business responsibilities.

Business Partner: Generally, a user belonging to a non-Commonwealth entity whose access to Commonwealth systems is required as part of a contract with or legal requirement placed on that entity.

CISO: Chief Information Security Officer of the Commonwealth of Pennsylvania.

Citizen: Any member of the public needing access to Commonwealth systems on their own personal behalf or on the behalf of their family or other dependents.

COTS: Commercial Off The Shelf. Software that can be procured and used with only minor customizations as opposed to custom built software.

Disable: An account may be disabled either by setting the 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.

GUID: Globally Unique Identifier is an alpha-numeric code which uniquely identifies a person. Two John Smiths, could for instance both have the same userID, but they would have different GUID's. User access to IT resources should be based on the GUID rather than the userID 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 which 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.

Multi-Factor Authentication: The use of two or more of the Authentication Methods (see above). Two-factor would employ one each of two of the methods; three-factor would employ one each of all three methods.

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

Passphrase: A password that is generated by a phrase or slogan that is more easily remembered by the user. E.g. "**Four S**core and **Seven Y**ears **a**go **o**ur **foref**athers **b**rought **forth** on **t**his **c**ontinent a **N**ew **N**ation" might translate to a password *4S7Yao4Fb4thtcNN*.

Password UserID/Name: use of the account userID or any part of the user's name in the password.

Permanence: indefinite lifetime of userID for as long as the person represented by the account remains active. This does not preclude the purging of the user store and the reuse of the userID for a different person so long as the GUID corresponding to the person is maintained indefinitely and is used by the applications.

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, work stations (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.

Resource Accounts: These accounts are typically used for scheduling of resources such as meeting rooms, projectors, and other devices. They may also serve as a group or facility (e.g. store) email account.

Risk-Based Authentication (RBA): A method of authentication that utilizes a risk profile to determine the proper authentication process.

Service Accounts: These accounts are typically used to authenticate one system or application to another. They may have "administrator" level privileges; they usually do not have an email address associated with them.

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.

System (non-Human) Accounts: These are assorted system accounts which are used for a variety of purposes. Generally, these accounts are used by systems or applications to communicate with one another or are general "shared" accounts used to facilitate working group activities.

Test User Accounts: These accounts are limited to non-production domains, though there are some instances where they are used in production to perform such functions as load-testing, service availability, and troubleshooting.

Training Accounts: These accounts are typically used for systems located in training room environments which may be accessible or used by multiple people.

Visibility: The display of a password in clear text, either during its entry, transmission to the end system, or in storage.

5. General Policy

Within thirty days of the date of issuance of this revised ITP, agencies will implement the specified access controls, as enumerated in this ITP, to standardize account ID and password controls in all computer systems and application environments. Multi-factor authentication (MFA) should be implemented for users requiring direct access to internal systems hosting/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 *§8.0 Reporting of non-Compliant Systems and Applications.*

New applications, whether COTS or wholly custom-built, that cannot employ the enterprise directories and cannot adhere to the account ID and password standards listed below will need to obtain a waiver to this ITP prior to going live (*§9.0 Exemptions and Waivers*) and will need to report these applications per *§8.0 Reporting of non-Compliant Systems and Applications.*

6. Detailed Policy

All computers or other devices, including hosted applications, permanently or intermittently connected to Commonwealth networks are to 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 to the Enterprise Information Security Office.

7. Reporting of non-Compliant Systems and Applications

In the case of non-compliant systems or legacy applications, the non-compliance will be reported to the agency security officer and the Commonwealth 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.

8. Exemptions and Waivers

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for a waiver is to be completed and submitted via the Commonwealth of Pennsylvania Policy and Procurement Action Request (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

The waiver request is to state why the standard user ID/password policy cannot be used. Details are required about the application, server, and network connections. Network diagrams are to be included to illustrate the security components that will mitigate the proposed user ID/password policy. *Any waiver that is granted will be valid for a period of not more than one (1) year and will be void if the application or system undergoes a substantial revision or replacement.* Despite the existence of the waiver, the non-compliant system or application is to be reported to the Commonwealth CISO as part of the agency's security assessment as prescribed above and detailed in ITP-SEC023 *Information Technology Security Assessment and Testing Policy*.

9. Related ITPs/Other References

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 - *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-SEC000 – *Information Security Policy*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC020 – *Encryption Standards for Data at Rest*
- ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*
- NIST Special Publication SP 800-118 - *Guide to Enterprise Password Management* (Draft)
- NIST Special Publication SP 800-63-2 - *Electronic Authentication Guideline*
- NIST Special Publication SP 800-53 Rev. 4 - *Security and Privacy Controls*
- NIST Federal Information Processing Standard (FIPS) 200 - *Minimum Security Requirements for Federal Information and Information Systems*

10. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

11. Publication Version Control

It is the 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 are to be directed to RA-ITCentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	09/07/2006	Base Policy
Revision	05/17/2010	Add language to address legacy applications
Revision	04/02/2014	ITP Reformat

		Merged RFD-SEC007A, RFD-SEC007B, RFD-SEC007C, BPD-SEC007D into ITP

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

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
Revision	12/15/2016	• Added GUID and Permanence definitions • Added ITP-SEC019 reference
Revision	12/07/2017	• Added definitions/language regarding inactive accounts and purging • Revised language throughout for clarity • Created OPD-SEC007A