pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Minimum Standards for IDs and Passwords

ITP Number	***Effective Date***
ITP-SEC007	March 1, 2006
Category	***Supersedes***
Security	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	May, 2016

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish minimum standards for the implementation and administration of user, system, network, device, and application account IDs and passwords.

Generally, the use of IDs and passwords 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.

The primary focus of this ITP is to provide minimum Account ID and Password standards. Multi-factor authentication techniques and standards required for certain applications and systems are out-of-scope though they may be required to supplement or to mitigate existing password policies.

3. Objective

The objective of this ITP is to:

- Provide security requirements for accessing computer applications, systems and data with UserIDs and passwords
- Provide a level of standardization and uniformity throughout Commonwealth of PA (COPA) agencies for UserID/Password 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.

CWOPA: Commonwealth of Pennsylvania Active Directory store for employees and contractors.

Enterprise Directories: Currently established user directory stores that are used by more than one agency for the purpose of authenticating users. Currently these are CWOPA (for employees and contractors), Managed Users (for business partners), and SRPROD (self-service for citizens and other "customers").

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.

Managed Users Directory: Enterprise Active Directory for "Business Partners", managed by the Department of Human Services.

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 Complexity: passwords will be constructed using characters from at least three of the following four character sets:

- Lower case letters: a, b, c, d, …, x, y, z
- Upper case letters: A, B, C, D, …, X, Y, Z
- Numbers: 0, 2, 3, 4, 5, 6, 7, 8, 9
- Special characters: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /

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

Permanence: indefinite lifetime of userID

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.

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.

SRPROD Directory: Enterprise Active Directory for "Citizens" managed by the Department of Human Services. Allows end users to self-register and manage their accounts.

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.

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.

The password needs to provide an adequate level of security, yet not be so complex that the user or administrator using the account takes the recourse of having to write it down or otherwise store it in an insecure fashion.

6.1 User Accounts

In accordance with the current commonwealth and/or agency PC/LAN Acceptable Use Policy, users are required to review and sign (physically or electronically) a user security agreement which:

- lists, or refers to the commonwealth employee's responsibilities relative to the use of the password, the commonwealth information accessed, and the equipment used (PCs or other information technology equipment)
- indicates that passwords and data are confidential
- all users are to sign the agreement to acknowledge their responsibilities

6.1.1. Enterprise Directory Services

Enterprise directory services are required to be utilized for user management and authentication for all enterprise and agency systems, unless not technically possible due to COTS implementation, legacy system limitations or other significant justification.

There are three enterprise directories managed by COPA or centers of excellence for production systems…

- CWOPA: Internal employees and contractors
- Managed Users: External: “business partners” and their employees
- SRProd: External “Citizens”

Corresponding directories are available for non-production development or test systems.

The following specifications for user IDs, Passwords, and Sessions apply to these enterprise directories:

User IDs:

	CWOPA	Managed Users	SRPROD
Maximum length	10	12	N/A
Uniqueness[1]	Yes	Yes	Yes
Permanence	Yes	Yes	Yes
Construction	Controlled by CUPSS[2]	Controlled by IdentityMinder[3]	User’s choice
Other	No whitespace[4]	No whitespace[4]	No whitespace[4]

[1] No two users can have the same user ID within the same user domain.

[2] The enterprise provisioning system creates the userID’s for employees and contractors. Generally this is the first initial and last name; contractors are prefaced by “c-“. UserID’s are limited to a maximum of 10 characters (including the “c-“ preface).

[3] The business partner provisioning system creates the userID’s for business partners. Generally this is the first initial and last name and is prefaced by “b-“. UserID’s are limited to a maximum of 12 characters (including the “b-“ preface).

[4] Whitespace characters include, but are not limited to, space (ASCII code 32) and TAB (ASCII code 9).

Passwords:

	CWOPA	Managed Users	SRPROD
Encrypted/Hashed	Stored and Transmitted	Stored and Transmitted	Stored and Transmitted
Null	No	No	No

Minimum length	8	8	8
Maximum length	255	255	255
Complexity	Yes[1]	Yes[1]	Yes[1]
UserID/Name	No[2]	No[2]	No[2]
Visibility	No	No	No
Re-Use	Last 10	Last 10	Last 10
Maximum lifetime	60 days	120 days	13 months
Minimum lifetime	15 days	15 days	15 days

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

6.1.2 Systems or Applications using non-Enterprise Directories

The following specifications for User IDs, Passwords, and Sessions apply to all other commonwealth or agency user stores (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 ITP's as dictated by the specific application or system.

User IDs:

Maximum length	50
Uniqueness[1]	Yes[1]
Permanence	Yes
Construction	N/A

[1] No two users can have the same user ID within the same user domain.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8
Maximum length	255
Complexity	Yes[1]
UserID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	60 days

Sessions:

Account lockout	After 5 failed attempts
Session inactivity	Lock PC after 15 min
Application inactivity	Logout after 10 hrs
Maximum session lifetime	Logout after 24 hrs

New applications and systems that cannot adhere to the standards listed above 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 and systems *(§8.0 Reporting of non-Compliant Systems and Applications*).
Recognizing that it may not be possible to enforce these minimum userID and password standards on such systems and applications, an exception to this policy may be granted where an agency can:

- Identify non-compliant system or application;
- Provide minimum user ID and password standards which are applicable to the platform and operating system or application in question which:
  - Are at least as strong as the above minimum standards, or
  - Are mitigated by other controls (e.g., requiring a Windows logon to access the terminal emulator).
- Non-compliant **legacy** systems will be grandfathered in, subject to the following condition:
  - The system must be reported to the Commonwealth CISO as prescribed below (§8 *Reporting of non-Compliant Systems and Applications*).
  - When the platform or application undergoes a substantial revision or replacement, the revised platform or application (or its replacement) will conform to the minimum user ID and password standards, integrating with the Commonwealth enterprise directories.

6.2. System (non-Human) Accounts

6.2.1. Service Accounts

Service Account IDs shall be requested, issued and deactivated via standardized processes. This is required to maintain a historical record of the Service Account and the timeframe during which the Service Account is/was valid. Access level or privilege level changes shall also be requested via standardized processes.

Service Account IDs and Passwords should be strategized and deployed in a diverse manner. For example, Service Account credentials for Application and Database access should vary for differing systems.

Service Accounts shall be established for system-to-system access. Anonymous system-to-system access is prohibited. Anonymous file transfer is prohibited.

System Administrators and other personnel must not use Service Accounts to directly access Applications, Databases, Servers, Routers or other systems. Initial account setup and related testing or debugging is permitted.

A record of production system testing where Service Accounts are used by System Administrators and possibly others shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

Service Accounts shall be reviewed on a regular basis not to exceed 180 days, to verify the appropriate distribution of credentials and access levels. A record for each review shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

Applicable system logs shall be reviewed on a regular basis not to exceed 180 days, to ensure that only authorized service accounts are being used to access systems, and to ensure that unauthorized access attempts are not occurring. A record for each review shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

Service Account passwords shall be issued in a secure manner and changed. on a recurring basis not to exceed 12 months.

Service Account passwords shall be changed as employees, contractors and other personnel having knowledge of the credentials, depart the organization or assume non-applicable roles.
Specific or unique service accounts should be created and use with the production environment.
Production service accounts should not be used in any other environment.

The following criteria are to be applied to service account IDs and passwords:

Account IDs:

Maximum length	50
Uniqueness[1]	Yes
Permanence	Yes
Construction	N/A

[1] No two accounts can have the same account ID within the same user domain.
Typically the service account is named to identify its agency and use.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8
Complexity	Yes[1]
Account ID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	12 Months

6.2.2. Resource Accounts

The following criteria are to be applied to resource account IDs and passwords:

Account IDs:

Maximum length	50
Uniqueness[1]	Yes
Permanence	Yes
Construction	N/A

[1] No two accounts can have the same account ID within the same user domain.
Typically the resource account is named to identify its agency and use.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8
Complexity	Yes[1]
Account ID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	N/A

6.3. Training Accounts

In training environments the account ID and password may be posted on the system for convenience. The following criteria are to be applied to training account IDs and passwords:

Account IDs:

Maximum length	50
Uniqueness[1]	Yes
Permanence	Yes
Construction	N/A

[1] No two accounts can have the same account ID within the same user domain. Typically the training account is named to identify its agency and location.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8
Complexity	Yes[1]
Account ID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	N/A

Where feasible, these accounts are to have restricted access to both the commonwealth MAN as well as the Internet. These accounts will have no access to any domain administrative functions on the PC or other equipment, including the ability to install software. Access to any type of sensitive information and/or ability to impact production systems is prohibited.

6.4. Test User Accounts

The following criteria are to be applied to Test User account IDs and passwords:

Account IDs:

Maximum length	50
Uniqueness[1]	Yes
Permanence	Yes
Construction	N/A

[1] No two accounts can have the same account ID within the same user domain. Typically the training account is named to identify its agency and location.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8
Complexity	Yes[1]
Account ID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	N/A

Their functionality is to be restricted to what is required by the application in question and they are not to have any local administrative functions on the PC.'s, Servers or other equipment unless specifically needed for testing purposes.

6.5. Privileged (System Administrator) Accounts

System Administrator IDs shall be requested, issued and deactivated via standardized process such as Service Now, CUPSS or other documented processes. This is required to maintain a historical record of the person associated with the System Administrator ID, and the timeframe during which the System Administrator ID is/was valid. Access level or privilege level changes shall also be requested via standardized process.

System Administrators shall have a unique user ID for system login that exclusively identifies the individual to whom it is assigned. The use of a strong password is also required, to protect against unauthorized use of another individual's user ID.

System Administrators are prohibited from logging into any system anonymously.

System Administrator IDs and Passwords must not be shared.

System Administrator ID's shall be reviewed on a regular basis, at least annually, to verify the appropriate distribution of credentials and access levels. A record for each review shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

Applicable system logs shall be reviewed on a regular basis not to exceed 180 days, to ensure that only authorized System Administrator accounts are being used to access systems, and to ensure that unauthorized access attempts are not occurring. A record for each review shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

System Administrator Passwords shall be issued and changed in a secure manner.

System Administrator IDs and Passwords shall be deactivated as employees, contractors and other personnel having credentials, depart the organization or assume non-applicable roles.

System administrators and others providing oversight for ID/Password administration shall review and sign non-disclosure per *Management Directive 245-18 IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures*.

System administrators shall not use their Administrator ID/Password for accessing the Internet and other such user-level activities. System administrators shall have a standard user ID/Password issued for such activities.

The following specifications for user IDs, Passwords, and Sessions apply to administrator accounts:

User IDs:

Minimum length	8
Maximum length	50
Uniqueness[1]	Yes
Reuse of network (CWOPA) user ID[2]	No
Permanence	Yes
Construction	N/A

[1] No two users can have the same user ID within the same user domain.

[2] The administrator will not use their general CWOPA userID or password for administrative access.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8

Complexity	Yes[1]
UserID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	60 days

Sessions:

Account lockout	After 5 failed attempts
Application inactivity	Logout after 10 hrs
Maximum session lifetime	Logout after 24 hrs

6.6. Privileged (Local Administrator) Accounts

Local Administrator account IDs shall be requested, issued and deactivated via standardized process. This is required to maintain a historical record of the person associated with the Local Administrator ID, and the timeframe during which the Local Administrator ID is/was valid. Access level or privilege level changes shall also be requested via standardized process.

Local Administrator IDs shall be strategized and deployed in a diverse manner for dissimilar systems. For example, Local Administrator IDs for Servers should be different from Local Administrator IDs for computer Work Stations.

Unless specified otherwise in this section, Local Administrators shall have a unique User IDs for system login that exclusively identifies the individual to whom it is assigned. The use of a strong password is also required, to protect against unauthorized use of another individual's user ID. Local Administrator IDs and Passwords must not be shared. Anonymous system login is not permitted.

Local Administrator accounts shall be reviewed on a regular basis, at least annually, to verify the appropriate distribution of credentials and access levels. A record for each review shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

Applicable system logs shall be reviewed on a regular basis not to exceed 180 days, to ensure that only authorized Local Administrator accounts are being used to access systems, and to ensure that unauthorized access attempts are not occurring. A record for each review shall be created and retained for an appropriate period as required by the appropriate enterprise or agency records retention schedule.

Local Administrator Passwords shall be issued and changed in a secure manner. Passwords shall be changed on a recurring basis not to exceed 180 days.

Where unique Local Administrator account IDs are assigned to individuals, Local Administrator IDs shall be deactivated as employees, contractors and other personnel assigned credentials, depart the organization or assume a non-applicable role.

The following two options are provided where significant difficulty may exist for implementing/assigning unique Local Administrator IDs and Passwords for each Administrator across a common platform:

- "Shared" Local Administrator ID and Password are permitted. However, the supervisor or manager having immediate oversight for applicable operations shall implement a process to ensure that a historical record is maintained, noting when Shared Local Administrator IDs and Passwords are used and by whom.
- Local Administrator passwords may be distributed ad-hoc. The supervisor or manager having immediate oversight for applicable operations shall retain and secure passwords, and distribute to subordinate staff as needed/ad-hoc. Upon completion of work, the passwords shall be changed, retained and secured by the supervisor or manager until needed again. The applicable supervisor or manager shall maintain a historical record, noting when Local Administrator IDs and Passwords are used and by whom.

Local Administrators and others providing oversight for ID/Password administration shall review and sign non-disclosure per *Management Directive 245-18 IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures*.

Local Administrators shall not use their Local Administrator ID/Password for using the Internet and other such user-level activities. Local administrators shall have a standard user ID/Password issued for such activities.

Local administrator accounts should be unique to the system/application environment. For example one local administrator account for Windows Servers, a different account for desktops, a different account for AIX servers, and so on.

The following specifications for user IDs, Passwords, and Sessions apply to local administrator accounts:

User IDs:

Minimum length	8
Maximum length	50
Uniqueness[1]	Yes
Reuse of network (CWOPA) user ID[2]	No
Permanence	Yes
Construction	N/A

[1] No two users can have the same user ID within the same user domain.

[2] The administrator will not use their CWOPA userID or password for non-administrative access.

Passwords:

Encrypted/Hashed	Stored and Transmitted
Null	No
Minimum length	8
Complexity	Yes[1]
UserID/Name	No[2]
Visibility	No
Re-Use	Last 10
Maximum lifetime	180 days

Sessions:

Account lockout	After 5 failed attempts
Application inactivity	Logout after 10 hrs
Maximum session lifetime	Logout after 24 hrs

6.7 General Password Policies

In accordance with commonwealth records-retention policy (*Management Directive 210.5 – The Commonwealth of Pennsylvania State Records Management Program*), maintain a historical record of all issued account IDs. This record is to identify the person associated with the user ID, and the timeframe during which the account ID is/was valid.

Multi-user systems are to employ unique user IDs and passwords, as well as user privilege restriction mechanisms. Network-connected, single-user systems are to employ hardware or software mechanisms that control system booting and include a no-activity screen blanker.

Computer and communication system access control is to be achieved via a minimum of user ID/password combinations that are unique to each individual user. Except where explicitly noted otherwise in Section 5.6 of

this ITP, Shared accounts or passwords are prohibited when the intent is to access files, applications, databases, computers, networks, and other system resources. Anonymous system login is not permitted.

Systems software is to be used to mask, suppress, or otherwise obscure all password fields to prevent the display, capture, and printing of passwords. Additional precautions may be necessary to prevent unauthorized parties from observing and/or recovering passwords. All passwords are to be encrypted or hashed both in storage and during transmission.

This policy does not prevent the use of default passwords--typically used for new user ID assignment or password reset situations--which are then immediately changed when the user next logs into the system.

Systems software is to limit validity of initial password(s) to the new user's first session log-on. At first log-on of a new account or after the password has been reset by an administrator or help desk, the user is to be required to choose a new password.

All vendor-supplied default passwords are to be changed before any computer or communications system is connected to a commonwealth network or used for commonwealth business. This policy applies to passwords associated with end-user IDs, as well as passwords associated with system administrator and other privileged users.

Incorrect password attempts are to be strictly limited, to prevent password-guessing attacks. Upon five (5) consecutive, unsuccessful attempts to enter a password, the involved account is to be suspended until reset by a system administrator. Reset process may be delegated to the Help Desk or similar function approved by Systems Administrator. When dial-up or other external network connections are involved, the session is to be disconnected. System administrators are to monitor access reports, logs and other system activity for login attempts and report discrepancies.

Data encryption is required for all electronic password repositories.

Whenever there is a convincing reason to believe that system security has been compromised, the involved system administrator is to immediately (a) reassign all relevant passwords and (b) require all passwords on the involved system to be changed at the time of the next login. If systems software does not provide the latter capability, a broadcast message is to be sent to all users instructing them to change their passwords. Additionally, the Enterprise Security Operations Team (security@pa.gov) is to be contacted and an incident report filed with the Enterprise Information Security Office.

Least privileged. By default all account should be assigned the lowest level of permissions. If elevated permissions are required a change request should be submitted and approved before elevated permissions are granted to any account.

6.8 General Password Recommendations

Passwords are an essential component of PC security. The more complicated the password, the more difficult it is for unauthorized users to gain access to an authorized user’s system.

Users are to choose passwords that are difficult to guess. Passwords are NOT to be related to a user’s job function or personal life. Users are not to incorporate a car license plate number, a spouse's name, or fragments of an address into their passwords. A password is to neither contain any word found in the dictionary, nor any proper names, places, technical terms, or slang. When available, systems software is to block and prevent usage of easily guessed passwords.

Users are to apply the following techniques to prevent unauthorized parties from guessing passwords. When choosing passwords:

- String several words together (the resulting passwords are also known as "pass-phrases").
- Shift a word up, down, left, or right one row on the keyboard.
- Bump characters in a word a certain number of letters up or down the alphabet.
- Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.
- Combine punctuation or numbers with a regular word.
- Create acronyms from words in a song, a poem, or another known sequence of words.
- Deliberately misspell a word (but not a common misspelling).

Users are not to construct passwords that are identical (or substantially similar) to previously employed passwords. When available, systems software is to block and prevent password reuse.

Users are not to construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users are NOT to employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

Readable-form passwords are not to be stored in: batch files, automatic login scripts, software macros, terminal function keys, computers without access control, or in other locations where unauthorized persons might discover them. Passwords are to be assigned to specific, authorized users and are not to be accessible by anyone other than the authorized user. Non-repudiation depends upon the unavailability of a password to anyone other than the authorized user. Administrator passwords can be archived in a secured location with access limited only to authorized users.

Passwords are not to be written down and left in a place where unauthorized persons might discover them, except for initial password assignment and password-reset situations. If there is reason to believe a password has been disclosed to someone other than the authorized user, the password is to be immediately changed.

Passwords are never to be shared or revealed to anyone but the authorized user, regardless of the circumstances. Revealing a password exposes the authorized user to the responsibility for actions that another party takes with the disclosed password.

7.0 Commonwealth of Pennsylvania Systems Log-In/Log-Off Process Policy

System and application administrators are to ensure that access to systems and data is authorized and to verify that a person or entity seeking access to systems and/or data is the one claimed. When authorizing access to systems and data, ensure that requestor has the minimum necessary access to perform required duties.

All users are to be positively identified and access levels verified, prior to granting access to data and prior to granting access to any applications, databases, communications system or other computer resources. Positive user identification for internal commonwealth networks involves both a unique user ID and password. The login process for network-connected commonwealth computer systems is to prompt the user to log in, providing additional prompts as needed. Specific information about the organization, the computer operating system, the network configuration, or other internal matters is not to be displayed until a user has successfully provided both a valid user ID and a valid password.

Positive identification for remote access (VPN) to commonwealth networked resources involves the use of hand-held tokens, cryptographic challenge/response, or other approved extended user authentication techniques. The

combination of a user ID and password does not provide sufficient security for remote connections to commonwealth systems or networks. Because modems do not provide adequate positive user identification, modems attached to network-connected workstations situated in commonwealth offices are forbidden, unless they are for dedicated uses. Examples of dedicated uses would include sending or receiving faxes, or connecting remote sensors to a central location. In these cases, care is to be taken to mitigate the risk presented by modems through the use of additional security layers: proper configuration, firewalls, DMZs, etc. Modems connected to isolated computers (portable computers and home computers) are permissible.

If there has been no activity on a computer terminal, workstation, or microcomputer for a certain period of time, the system is to automatically blank the screen and suspend the session. Re-establishment of the session is to take place only after the user has provided a valid password. The period of time is not to exceed fifteen (15) minutes. An exception to this policy will 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.

Users are prohibited from logging into any commonwealth system or network anonymously (for example, using "guest" user IDs). Users are to initially log-in with a userID that clearly indicates their identity, when using systems facilities that allow changing the active userID to gain certain privileges. On UNIX systems, users are prevented from initially logging in as "root," and are to first log in using their own userID.

Whatever the operating system, logs are to record all changes in current user IDs. Electronic bulletin boards, or other systems where all regular users are anonymous, may be a permissible exception.

8.0 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.

9.0 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 semi-annual security assessment as prescribed above.

10.0 Related ITPs/Other References

- ITP-SEC020 – Encryption Standards for Data at Rest.
- ITP-SEC023 – Information Technology Security Assessment and Testing Policy
- 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
- 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-800-53-4, Security and Privacy Controls
- NIST Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems

11.0 Authority

Executive Order 2011-05, Enterprise Information Technology Governance

12.0 Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. 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	9/7/2006	Base Policy
	7/16/2009	Updated: minimum number of password characters to eight
	5/17/2010	Add language to address legacy applications
	7/26/2010	User lockout feature changed from 3 unsuccessful login attempts back to 5 attempts due to a multitude of technical issues: Note: This change is temporary until issues are resolved.
	6/19/2012	Revised the user ID requirements to exclude use of whitespace; require waivers for any agency using non-conforming user account repositories for application or system authentication.
	4/2/2014	ITP Reformat; Merged RFD-SEC007A, RFD-SEC007B, RFD-SEC007C, BPD-SEC007D into ITP

Revision	05/05/2015	• Rewrite of Purpose section
		  o Added Systems
		  o Added Peripheral equipment
		• Expanded and clarified Scope section
		• Expanded and clarified Objective section
		• Added Definitions section
		• Expanded:
		  o Section 5 General Policy
		  o Section 6 Detailed Policy
		• Categorized Detailed Policy sections
		  o User Accounts
		  o Enterprise Directory Services
		  o Systems or Applications using non-Enterprise Directories
		  o System (non-Human) Accounts

		▪ Service Accounts ▪ Resource Accounts o Training Accounts o Test User Accounts o Privileged (System Administrator) Accounts o Privileged (Local Administrator) Accounts • Added Specifications Tables for (where applicable) o User IDs o Passwords o Sessions • Added General Password Policies and Recommendations • Revised language in CoPA Systems Log-In/Log-Off Process Policy Section 7 • Added Reporting of non-Compliant… as its own section (Section 8) • Expanded Related ITPs/Other References Section 10