pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Minimum Standards for User IDs and Passwords

ITP Number ITP-SEC007	***Effective Date*** March 1, 2006
Category Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

This Information Technology Policy (ITP) establishes policy for the minimum standards of user IDs and passwords.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish policy regarding the minimum standards for establishment of user IDs and secure passwords.

Generally, the use of user IDs and passwords provides for Authenticated and Authorized access to:

- The enterprise LAN/WAN
- Enterprise applications (e.g., Exchange, VPN)
- Agency applications

It also provides the capability to audit the activities of users in these systems.

These capabilities require, at a minimum, a unique user ID 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. The password needs to provide an adequate level of security, yet not be so complex that the user takes the recourse of having to write it down or otherwise store it in an insecure fashion.

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

To establish policy for the minimum standards of user IDs and passwords.

4. Policy

All computers permanently or intermittently connected to commonwealth networks, including portable devices, are to have minimum user ID and password access controls.

Systems Running the Windows Operating System

At the enterprise level, user IDs and passwords are controlled through the policies governing

the Commonwealth of Pennsylvania (CWOPA) Active Directory. Details of these policies may be obtained upon approval of an application submitted to the Commonwealth Chief Information Security Officer (CISO).

Within thirty days of the date of issuance of this ITP, agencies will implement the specified access controls, as presented in the documents listed below, to standardize user IDs and passwords in all computer systems and application environments including, but not necessary limited to, desktops, notebooks, LANs, and networks.

In addition, the agencies are to:

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

- In accordance with the current commonwealth and/or agency PC/LAN Acceptable Use Policy, review and require users to 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), as outlined in the applicable commonwealth and agency PC and Internet acceptable use policies
    - indicates that passwords and data are confidential
    - all users are to sign the disclaimer(s) to acknowledge their responsibilities
- Maintain the same minimum policies for any agency-level Active Directory or any other user repository.

Systems Running Other Operating Systems

There are numerous other operating systems within the commonwealth, including those supporting hand-held and other mobile devices, mainframes, network devices, and other non-Windows computing systems. These include, but are not limited to, Macintosh, Linux, UNIX, SUN/Solaris, AS400, Unisys OS, RACF, Cisco IOS, Nokia IPSO, and Checkpoint firewall systems. Recognizing that it may not be possible to enforce the above Windows-based minimum user ID and password standards, an exception to this policy may be granted for such systems where an agency can:

- Identify the non-Windows system;
- Provide minimum user ID and password standards which are applicable to the platform and operating system in question which are:
    - at least as strong as the above Windows minimum standard, or
    - supplemented by other procedures (e.g., requiring a Windows logon to access the terminal emulator).
- Such non-compliant systems will be grandfathered in, subject to the following condition:
    - The system must be reported to the Commonwealth CISO as prescribed below

Legacy Applications

There are numerous legacy applications within the commonwealth, including those supporting mission critical agency functions. These may have been written years ago in COBOL or other such programming languages which now have limited support for maintenance or updates. Recognizing that it may not be possible to enforce the above Windows-based minimum user ID and password standards, an exception to this policy may be granted for such systems where an agency can:

- Identify the legacy application;
- Provide minimum user ID and password standards which are applicable to the application in question which are:
    - at least as strong as the above Windows minimum standard, or
    - supplemented by other procedures (e.g., requiring a Windows logon to access the terminal emulator).
- Legacy applications will be grandfathered in, subject to the following conditions:
    - The application must be reported to the Commonwealth CISO as prescribed below
    - At such time as the application is undergoing a substantial revision or replacement, the revised application (or its replacement) will conform to the Windows-based minimum user ID and password standards, integrating with the Commonwealth enterprise active directories.

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 Commonwealth CISO as part of the agency's semiannual security assessment (ITP-SEC023). 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 mitigating circumstances or practices, and any plans for the revision or replacement of the system or application.

5. Commonwealth of Pennsylvania Detailed Windows Password Policy

Password policies for the enterprise Windows environment are controlled through the CWOPA Active Directory. These policies include user identifications (IDs) and passwords.

User IDs:

- Must be a maximum of ten characters.
- Are unique. No two users can have the same user ID within the same user domain.
- Are permanent. They may be disabled and retired, but they are not to be reused.
- Often take the form of the user's first initial plus last name, subject to the above restrictions. Variations are allowed, as required, to generate a unique user ID.
- Are different for contractors. Contractors' user IDs are prefaced with "c-", followed by the first initial, last name, etc., as above, with the total number of characters, including "c-", limited to the maximum ten characters.
- May not contain any whitespace character either leading, trailing, or within the user ID. Whitespace characters include, but are not limited to, space (ASCII code 32) and TAB (ASCII code 9).

Passwords:

- Must not be NULL
- Must be a minimum of eight characters.
- Must be composed of at least three of the following types of characters:
  - Uppercase letters (A, B, C, …)
  - Lowercase letters (a, b, c, …)
  - Numbers (0, 1, 2, 3, …, 9)
  - Special characters (#, other punctuation marks).
- May neither contain the user ID, nor any part of the user's full name.
- May not reuse any of the last ten previously used passwords.
- Will expire after sixty days, requiring the creation of a new password.
- May not be changed more than once every fifteen (15) days.

User IDs are locked after five (5) consecutive failed log-on attempts and require administrator-level access to unlock them. In addition, once a user is logged in, the system will be locked after fifteen (15) minutes of inactivity, requiring the user to re-enter the password to regain access to the system. Agencies may apply more stringent requirements as dictated by their environment and their applications.

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. Service accounts are also permitted; however, their use should be strictly limited and their passwords changed on a regular basis.

6. Commonwealth of Pennsylvania Password Administration Policy

All computers permanently or intermittently connected to commonwealth networks, including portable devices, are to have password access controls. 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 user ID/password combinations that are unique to each individual user. Shared accounts or passwords are prohibited when the intent is to access files, applications, databases, computers, networks, and other system resources.

Systems software is to be used to mask, suppress, or otherwise obscure password fields to prevent the display and printing of passwords. Additional precautions may be necessary to prevent unauthorized parties from observing or recovering passwords.

Systems software is to limit validity of initial password(s) to the new user's first session log-on. At first log-on, the user is to be required to choose a new password. This same process applies to the resetting of passwords.

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 user ID is to be suspended until reset by a system administrator. When dial-up or other external network connections are involved, the session is to be disconnected.

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. The Enterprise Security Team (security@state.pa.us) is to be contacted.

7. Commonwealth of Pennsylvania Systems Log-In/Log-Off Process Policy

All users are to be positively identified prior to being able to use any multi-user computer or communications system resource.

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 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 a password does not provide sufficient security for remote connections to commonwealth systems or networks. Therefore, 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.

Positive identification for users establishing external, real-time connections into commonwealth systems or networks via value-added public networks, or any other external communications system, is to also involve sophisticated user authentication techniques.

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 recommended 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. 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 that would be difficult for unauthorized parties to guess, 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.

9. Exemptions

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. Related ITPs/Other References

- ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*

11. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

12. 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