

**COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE
INFORMATION TECHNOLOGY POLICY**

Name Of Policy: User Identity and Access Management	Number: POL-SEC012
Domain: Security	Category:
Date Issued: 05/23/11	Issued By Direction Of:
Date Revised: 11/14/13	 Sandra Patterson, CIO Bureau of Information Systems

Table of Contents

1	Introduction	3
1.1	Purpose	3
1.2	Scope	3
1.3	Compliance	3
1.4	Exemptions.....	3
1.5	Policy Review and Update	3
2	User Identifier (UserID) Management.....	3
3	Password Management	4
4	Session Management and System Use Notification.....	5
5	Access Enforcement	6
6	User Account Administration	7
7	Appendix	8
7.1	References.....	8

Document History

Version	Date	Author	Status	Notes
1.0	05/23/2011	Tom Zarb	Draft	Initial Creation
1.1	11/14/2013	John Miknich	Draft	Revision & Updation

1 Introduction

1.1 Purpose

This policy addresses how access to DPW information and information systems is controlled; including the identification, authorization and authentication of users, programs and processes that access DPW information resources. This policy also addresses compliance with DPW, federal and Commonwealth of Pennsylvania (CoPA) requirements.

1.2 Scope

All DPW employees, contractors and other stakeholders are responsible for understanding and complying with this policy, and as applicable, the supporting policies, standards, and procedures.

1.3 Compliance

All DPW employees, contractors and other stakeholders are expected to be familiar with and comply with this policy. Violations of this policy can lead to revocation of system privileges and/or disciplinary action.

1.4 Exemptions

Any exemptions to this policy must be approved by the Chief Information Security Officer (CISO).

1.5 Policy Review and Update

This document, and its supporting policies, standards and procedures, shall be reviewed annually and updated as needed.

2 User Identifier (UserID) Management

User identifier management addresses proper use of credentials for the unique identification and authentication of users.

DPW Policy

General

- a. All DPW web applications shall uniquely identify and authenticate users (or processes acting on behalf of users).
- b. All DPW information systems and applications shall be protected using guidelines specified in Commonwealth's Information Technology Bulletins ITB SEC013, *Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services* and ITB-SEC014, *Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Technology Standards*.
- c. System Owners shall ensure that User Identifiers are implemented and maintained that support access control, least privilege, and system integrity.
- d. DPW users shall not share UserIDs and passwords.
- e. Any use of a group UserID and password shall be limited to situations dictated by operational necessity, and must be approved in writing by the CISO.

CoPA Users and Contractors

- f. Standards governing UserID management for CoPA information systems are provided in Information Technology Bulletin (ITB)-SEC007, Minimum Standards for UserIDs and Passwords.

DPW Business Partners

- g. The naming convention for the creation of new UserIDs includes:

DPW Policy

- The UserID shall contain a maximum of 12 characters and begin with 'b-'
 - The UserID creation is automated. The system shall use one or more letters of the user's first name and last name to create a unique UserID (For example, a user 'John Smith' may be provided the UserID 'b-jsmith', based on availability)
 - Business partner user accounts shall be created in the "Managed" active directory only.
- h. Minimum information requirements to create a business partner user account are:
- First name and last name.
 - Business partner organization Federal Employer Identification Number (FEIN).
 - Email address. The email address must be unique for each individual business partner account.
 - Electronic acceptance of the Management Directive (MD) 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy
- i. The business partner user account shall be approved by either the corresponding program office administrator or the business partner's delegated administrator.

Citizen Users

- j. The naming convention for the creation of new citizen user account includes:
- The UserID shall contain a maximum of 12 characters
 - The UserID shall be selected by the end user
 - The citizen user accounts shall be created in the "SRPROD" active directory only.
- k. Minimum information requirements to create a citizen user account are:
- First name and last name.
 - Date of Birth
 - Security Question / Answer
 - Electronic acceptance of the appropriate application's usage terms and conditions.

3 Password Management

Password management is the enforcement of a set of rules or laws that govern the creation and lifecycle of passwords. Effective password management is critical to controlling and securing access to protected information.

DPW Policy

General

- a. Program Offices/System Owners shall ensure that information systems protect passwords from unauthorized disclosure and modification when stored and transmitted.
- b. Program Offices/System Owners shall ensure that passwords are not displayed when entered (e.g., asterisks are displayed when a user enters a password).
- c. Program Offices/System Owners and the DPW security administrator shall replace all default passwords provided by the vendor.
- d. Program Offices/System Owners shall ensure that upon a user entering incorrect or incomplete password information, the feedback error message states, for example, "UserID or password entered

DPW Policy

is invalid".

CoPA Users and Contractors

- e. Policy governing password management for CoPA information systems is provided in ITB-SEC007, Minimum Standards for UserIDs and Passwords.
- f. The maximum number of unsuccessful logon attempts for DPW applications is three

DPW Business Partners and Citizen Users

- g. Minimum password requirements for business partners and citizen users include:

Password Length	Passwords must be a minimum of eight characters
Password Complexity	<ul style="list-style-type: none"> o Passwords must contain characters from at least three of the following four categories: uppercase letters; lowercase letters; 0-9 (numbers); and, non-alphanumeric characters (such as !,<,@,# or \$) o Passwords may neither contain the UserID, nor any part of the user's full name o Passwords may not be changed more than once every two days.
Password Reuse Limit	Users may not reuse any of the last ten previously used passwords.
Password Expiration	<p>Business Partners</p> <ul style="list-style-type: none"> o Passwords shall expire after 60 days. o After 60 days of inactivity, users have to follow the department's password reset process to enable access to the DPW applications. <p>Citizen Users</p> <ul style="list-style-type: none"> o Passwords shall expire after 270 days (9months). o After 270 days of inactivity, users have to follow the department's password reset process to enable access to the DPW applications.
Password Display	Systems shall mask, suppress, or otherwise obscure password fields to prevent the display and printing of passwords.
Unsuccessful Logon Attempts	UserIDs are locked after three consecutive failed log-on attempts and require administrator-level access to unlock them.
Account Lockout	<ul style="list-style-type: none"> o Accounts are automatically locked after 13 months of inactivity o Permanently revoked UserIDs are not to be reissued. o UserIDs shall not be deleted from the Active Directory.

4 Session Management and System Use Notification

DPW requires that all communications sessions between components of information systems or between information systems themselves be both authenticated and actively managed. This includes monitoring, suspending, disabling and terminating communications to and from information systems. Without session management, the potential exists that communications can be established or used illegitimately, thereby exposing information to an increased likelihood of loss or corruption.

DPW Policy

General

DPW Policy

- a. DPW provides and implements password-protected screen savers on all workstations used by DPW stakeholders. The screen saver shall automatically lock the workstation after fifteen minutes of inactivity. Program Offices/System Owners of moderate- or high-impact systems shall require that contractors and business partners who connect to the systems implement such a screen saver.
- b. DPW web applications and services shall have a default timeout of 20 minutes. Once a user is logged in, the system shall time-out after 20 minutes or upon BIS approved time period of inactivity, requiring the user to re-enter the password to regain access to the system.
- c. DPW web applications shall encrypt sessions using Secure Sockets Layer (SSL) v3 or Transport Layer Security (TLS) v1 with at least 128-bit key length.
- d. DPW's VPN shall have a default timeout (upon successful authentication) of four hours.
- e. DPW system's remote desktop sessions shall allow a maximum of two concurrent active sessions.
- f. For DPW web applications, Secure Sockets Layer enabled HTTP-only session cookies shall be used.
- g. At the time of logon, the system or the application shall display a message consistent with the requirements of ITB-SEC012, Commonwealth of PA System Logon Banner Requirements Policy.

5 Access Enforcement

Access enforcement addresses how access to information resources is determined, granted and enforced. These minimum security requirements shall be established during the design phase of the system development lifecycle, as well as during the implementation and maintenance phase.

DPW Policy**General**

- a. All users shall ensure that their unattended workstations are either logged off or locked, or that a password-protected screensaver is used.
- b. Program offices and system owners shall ensure that their information systems implement access control measures to provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.
- c. Guest/anonymous accounts are not to be used. Default vendor or factory-set administrator accounts and passwords shall be changed before installation or use on DPW systems.
- d. Program offices and system owners shall ensure that users of information systems under their purview have approved access requests prior to granting access to the systems. Program Offices/System Owners shall ensure that user access is reviewed once a year.
- e. Program Offices and system owners shall ensure that individual users using administrative accounts/access shall read and sign the Commonwealth's IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures (MD245.18) annually.

Least Privilege

- f. Each DPW user, program or process shall be granted only the access specifically needed to perform assigned duties.
- g. User access to DPW applications, systems and information shall be based on the principle of least privilege.

Need to know

- h. Access to DPW information resources must be granted only when specifically authorized, based on job function and responsibilities.
- i. Granting or changing user access shall require written or electronic verification by the corresponding

DPW Policy

supervisor, based on the principle of need-to-know.

Default to deny

- j. User access to DPW applications, systems and information shall be based on the principle of default deny.
- k. By default, each DPW user, program or process shall be denied access to the department's systems.
- l. By default, granting or changing user access shall be denied and the protection scheme identifies conditions under which access is permitted.
- m. Anything that is not pre-approved, allowed or whitelisted is for all purposes blocked, denied or blacklisted.

Separation of Duties

- n. To reduce the risk of accidental or deliberate system misuse, DPW shall implement and enforce separation of duties mechanisms where practical.
- o. Whenever separation of duties is difficult to achieve, other compensatory controls such as monitoring of activities, audit trails and management supervision shall be implemented.

Public Available Information

- p. DPW shall designate staff to review and approve publically accessible content prior to publication
- q. DPW designated staff shall be review publicly accessible information to ensure that it does not contain sensitive data categories as defined by the department's web application privacy standard STD-ENSS034.

6 User Account Administration

The management of information system accounts includes identifying authorized information system users and specifying corresponding access privileges; and establishing, activating, modifying, disabling, and removing accounts.

DPW Policy

General

- a. DPW user accounts (Commonwealth user accounts) shall be managed only by select authorized individuals within or on behalf of the Bureau of Information Systems (i.e., Security Architecture Section's account administration team).
- b. Access to DPW information systems shall be approved by the appropriate system owner and/or the data owner.
- c. DPW shall review information system accounts within every one-hundred-eighty (180) days and require annual certification.
- d. DPW information system shall have centralized mechanisms to automatically audits account creation, modification, enabling, disabling, and removal actions, and report.
- e. The organization shall require multi-factor authentication for consumption of privilege user accounts.
- f. DPW shall review information system administrator access at least once every 14 days.

DPW Web Applications

- g. Access to DPW web applications shall be approved by the appropriate program office accounts after 48 hours.

DPW Policy

- h. DPW web application user accounts shall be managed only by the Security Architecture Section's account administration team, appropriate help desk or the corresponding business partner delegated administrator. For DPW business partners, user accounts shall be managed by the respective program office.
- i. Access permissions to delegated administrators for account management shall be restricted to their corresponding business partner organization and reviewed annually by the corresponding program office.
- j. DPW user account management processes include the following sub-processes:
- Identifying and enrolling new authorized information system users
 - Specifying access privileges
 - Establishing and activating accounts
 - Modifying accounts
 - Password reset processing
 - Disabling and removing accounts
- k. DPW shall automatically terminate temporary and emergency accounts after 48 hours.

7 Appendix

7.1 References

Document	Type
User Identifier and password Management	
Identity and Access Management for Web Applications	DPW policy
Identity and Access Management Service Accounts	DPW policy
Identity and Access Management Implementation Guidelines	DPW Guideline
ITB-SEC007 - Minimum Standards for UserIDs and Passwords	COPA Standard
ITB-SEC013 - Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services	COPA Policy
ITB-SEC014 - Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Technology Standard	COPA Standard
Access Enforcement	
DPW Role Based Access Control Project, Role Lifecycle Management	DPW Standard
Identity and Access Management Implementation Guidelines	DPW Guideline

Document	Type
User Account Administration	
Identity and Access Management Implementation Guidelines	DPW Guideline
Identity and Access Management Service Accounts	DPW Policy
ITB-SEC007- Minimum Standards for UserIDs and Passwords	CoPA Standard
ITB-SEC013 - Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services	CoPA Policy
ITB-SEC014 - Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Technology Standards	CoPA Standard