pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-005

Name:	Identification and Authentication of Users on L&I Systems
Effective Date:	July 2017
Category:	Security
Version:	2.2

1. Purpose:

This policy provides direction for Office of Information Technology (OIT) staff to support the business of Department of Labor & Industry (L&I) by providing secure access and authentication to L&I systems. This policy establishes a password management strategy for L&I. This policy documents the required attributes of user ID and passwords that control access to L&I systems. This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-1, AC-2, AC-3, IA-1, IA-2, and SC-23 Per SP 800-53 R4.

2. Background:

The L&I OIT has implemented and is maintaining a program to adequately secure information and system assets in support of L&I missions and Commonwealth enterprise goals and objectives. The program ensures that L&I systems and applications operate effectively; provides appropriate confidentiality, integrity, and availability; and protects information commensurate with the level of risk and magnitude of harm that may result from unauthorized access, use, disclosure, modification or destruction.

User IDs and passwords are primary and basic controls over access to L&I systems. A poorly designed/created password may result in the compromise of L&I systems.

3. Scope:

This policy applies to all employees within all bureaus, divisions, boards, commissions, and councils within L&I. This includes any contracted employees in the service of L&I. (hereinafter referred to collectively as "L&I Users")

4. Policy:

All applications must authenticate and manage user accounts and passwords in either the Commonwealth of PA (CWOPA) domain Active Directory (AD), Managed AD for businesses, or (Self-Registered) SR AD for citizen accounts. Legacy (mainframe) applications and systems that use alternative user management methodologies must comply with the minimum user ID and password standards established in Office of Administration(OA) ITP SEC007.

All system owners shall define roles and the permissions for the roles used in the application.

OIT shall design and configure all applications to comply with user ID and password standards as defined in OA ITP SEC007.

OIT shall conduct internal reviews to assess privileged user permissions and dormant account status, according to the data owner's requirements.

All L&I Users shall ensure the confidentiality of their user credentials and shall not share their password with anyone, including OIT or helpdesk staff. OIT and helpdesk staff may not request an L&I User's credentials.

L&I Users shall report any request for their credentials to the L&I Information Security Officer.

L&I Users shall be responsible for all activities conducted by their user ID.

L&I Users shall not request another user's user ID or password for any reason.

L&I Users shall ensure separation actions are processed for subordinates and contracted staff.

5. Responsibilities:

A. L&I User responsibilities:
- Ensure the confidentiality of their user credentials;
- Protect and secure IT equipment;
- Comply with all L&I policies, management directives, and laws; and
- Report any violations of policies promptly to the L&I Information Security Officer at LI, OIT-DLICISO.

B. L&I management responsibilities:
- Comply with all L&I policies and ensure L&I users comply with the policies; and
- Adhere to this policy and any published procedures regarding identification and authentication of users on L&I systems.

6. References:

L&I Policy Definitions Document

SEC-004 - Computer and Information Security

ITP SEC007 - Minimum Standards for User IDs & Passwords

7. Version Control:

Version	Date	Purpose
1.0	07/2007	Base document
2.0	06/2014	Policy update
2.1	05/2016	Updated to new policy format
2.2	07/2017	Annual review & content revision