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 New L&I Computer Systems |
| **Effective Date:** | May 2016 |
| **Category:** | Security Domain |
| **Version:** | 2.1 |

## 1. Purpose:

The purpose of this policy is to establish a password management strategy for the Department of Labor & Industry (L&I). This policy will document the required attributes of user ID and passwords that control access to L&I systems.

## 2. Background:

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, contractors, temporary personnel, members of boards, commissions and councils, agents and vendors in the service of L&I.

## 4. Policy:

The L&I Office of Information Technology (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. A critical component of the program is ensuring that systems and applications operate effectively, provide appropriate confidentiality, integrity, and availability, and information is protected commensurate with the level of risk and magnitude of harm that may result from its unauthorized access, use, disclosure, modification or destruction.

All applications must authenticate and manage user accounts/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) policy ITP SEC007.

Users are responsible for ensuring the confidentiality of their user credentials and are prohibited from sharing them. Users are responsible for all activities conducted by their user ID. Employees and contracted resources are never to request another user's user ID or password for any reason.

L&I OIT will design and configure all applications to comply with user ID and password standards as defined in the OA policy ITP SEC007.

## 5. Responsibilities:

Any information security breaches must be reported immediately upon discovery to L&I's Enterprise Security and Compliance section chief.

A. Employee and other user responsibilities:

- The confidentiality of their user credentials
- Protecting and securing assigned IT equipment
- Complying with all security policies, management directives and laws

B. L&I management responsibilities:

- Understand the risks of compromised data
- Understand all L&I policies and ensure employees understand the policies

**6. References:**

L&I Policy Definitions Document

L&I 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 |