pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-013

Name:	Access Management
Effective Date:	June 2017
Category:	Security
Version:	1.1

1. Purpose:

The purpose of this policy is to create a prescriptive set of processes, procedures, and training, aligned with applicable Governor's Office of Administration (OA) and the Department of Labor & Industry (L&I) Information Technology (IT) security policies and standards. This policy identifies guidelines for identity and access management at L&I. This policy establishes controls for designing and implementing access security and procedures for user credential management. This policy provides direction for users to gain additional access to systems and manage their credentials. This policy will help protect information, including Federal Tax Information (FTI), from unauthorized access and improper disclosure in compliance with safeguards and requirements defined by the Internal Revenue Service (IRS) and the Social Security Administration (SSA). This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-1, 2, & 3 Per SP 800-53 R4.

2. Background:

This policy is published under the general authority of the Governor's Office of Administration / Office of Information Technology (OA/OIT)

Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. Properly authenticating and granting access to users is tightly integrated with the security and productivity of any organization involved in electronic commerce. Having a mature IAM solution can improve performance of a service or application by automating tasks; enabling citizens, business partners, and staff to securely access information; and providing regulatory compliance.

L&I primarily uses Active Directory structures and Resource Access Control Facility (RACF) to control access to applications and 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:

A. General

OIT shall architect solutions using the least privilege model that will not result in the leakage of permissions or data to an unauthorized user.

L&I's Office of Information Technology (OIT) shall implement Role Based Access Controls (RBAC) to grant and restrict access to sensitive data.

OIT shall control the granting of elevated privileges to user accounts following the IT Access Management plan.

OIT shall only process access management changes with the approval of the L&I User's management.

OIT shall document all requests for access using the Information Technology System Management (ITSM) tool following L&I change control processes and procedures.

All L&I Users with elevated privileges shall annually sign the Acceptable Use Policy Agreement for System/Infrastructure/Database/Application Administrators OIT-8.

All L&I Users shall be responsible for all activity that is conducted by their assigned user ID.

OIT shall conduct internal audits of all access management control systems. Internal audits shall be used to determine access capabilities, inherited privileges, and separation of duties per APP-000 and SEC-012.

OIT shall develop and document procedures to revoke elevated privileges. OIT shall develop procedures to "lock" user accounts based on approval from the agency Chief Information Officer/Deputy Chief Information Officer (CIO/DCIO), Employee Relations, or the agency security officer or security chief.

B. Active Directory

OIT shall follow policies and controls implemented by OA/OIT.

L&I Users shall follow the change management process to change their access permissions.

C. RACF

All requests for RACF user IDs/additional resources shall be submitted through the ITSM tool. L&I Users shall follow the change management process to change their access permissions.

All RACF user IDs shall be associated with the L&I User's proper name. If an L&I User's proper name changes, that L&I User shall request a user ID change following the change control process as soon as possible.

L&I Users shall maintain confidentiality of data as required by law.

L&I Users shall adhere to the password lifetime controls.

L&I Users shall adhere to OA ITP-SEC007 concerning the security of user credentials and passwords.

L&I Users shall notify their supervisor and CISO if they think their password has become known to anyone else.

L&I Users shall not automate or script a sign on procedure for RACF, as this represents a disclosure of user credentials and passwords.

OIT shall revoke user IDs after five consecutive unsuccessful logon attempts or after 90 days of inactivity.

L&I Users shall use the ITSM tool or help desk to request the reactivation of a revoked user ID.

5. Responsibilities:

A. L&I User responsibilities:

- Comply with all L&I policies, management directives, and laws; and
- Report any violations of policies promptly to the L&I Chief 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 configuration management.

6. References:

L&I Policy Definitions Document

ADM-002 - ITIL Compliance

SEC-000 - Security Planning Policy

SEC-004 - Computer and Information Security

SEC-010 - Access Control for Non-Commonwealth Users Policy

SEC-012 – Audit, Accountability, and Reporting Policy

OA ITP-SEC007 Minimum Standards for IDs, Passwords, & Multi-Factor Authentication

OA ITP-SEC013 IPAM Identity Management Services

OA ITP-SEC014 IPAM Identity Management Technology Standards

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base Document
1.1	05/2017	Format and Content Revision