pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SYM-002

Name:	Configuration Management Policy
Effective Date:	March 2017
Category:	System Management
Version:	1.2

1. Purpose:

This policy provides directions and identifies guidelines for configuration change control, and access restrictions for changes within the Department of Labor & Industry (L&I). This policy provides direction for security impact analysis, configuration settings, establishes least functionality, and establishes standards for baseline configurations. This policy also fulfills the requirements of Internal Revenue Service (IRS) Publication 1075 safeguards and the requirements defined by the Social Security Administration (SSA). This policy documents the implementation of NIST Security Controls: CM-1, 2, 3, 6, 7, & 9, and SA-10.

2. Background:

This policy is published under the general authority of the Governor's Office of Administration / Office of Information Technology (OA/OIT) in conjunction with IRS Publication 1075 in that it identifies key roles and responsibilities regarding configuration management. IRS Publication 1075 provides direction regarding acceptable configuration management standards to help ensure that the agency is functioning consistently and at peak efficiency.

Configuration management controls help define the security state of the agency and infrastructure. These controls are also used by auditors to determine compliance.

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:

L&I Office of Information Technology (OIT) is responsible for establishing controls for the configuration of all systems, and IT Equipment.

A. Baseline Configuration

L&I OIT shall maintain a log of Baseline Configuration assessments initiated and completed.

L&I OIT shall use the Information Technology Service Management (ITSM) tool as the system of record.

L&I OIT shall document connectivity and data flows for each system, including network topology and the logical placement of components within each systems' architecture.

L&I OIT shall establish Baseline Configurations, including:

- registry settings;

- account, file, directory permission settings; and
- settings for functions, ports, protocols, services, and remote connections.

L&I OIT shall annually review baseline configurations of information systems to ensure the documentation reflects the current enterprise architecture as part of L&I OIT SYM-001.

B. Configuration Change Control

All configuration changes shall comply with L&I's established change control process. Configuration changes shall comply with L&I's System Development Life Cycle (SDLC) policy.

L&I OIT shall maintain records in the ITSM tool of all changes that impact entire systems or cross multiple systems including enterprise wide changes.

L&I OIT shall conduct audits of configuration changes as part of the Release Management and Service Validation processes.

C. Access Restrictions for Change

L&I OIT shall permit only authorized users to access information systems for purposes of initiating changes, including upgrades and modifications.

L&I OIT shall maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should L&I OIT discover any unauthorized changes.

L&I OIT shall restrict access to software libraries, abstraction layers, and application configuration in accordance with the L&I SDLC.

L&I OIT shall ensure physical security by implementing physical security controls and barriers, authorizing and vetting access to restricted workspaces of OIT per SEC-006 and SEC-010 and NIST Security Controls.

L&I OIT shall restrict access to databases using workflow automation and limited permissions for user accounts.

D. Configuration Settings

L&I OIT shall standardize configuration settings for servers, workstations, and mobile devices.

L&I OIT shall implement automated tools to manage the deployment of configuration changes.

L&I OIT shall document existing configuration and security settings for all Commercial Off The Shelf (COTS) products, internally developed applications, databases, operating systems, and hardware devices, including scanners, copiers, printers, network equipment, wireless access points, network appliances, and sensors.

L&I OIT shall implement monitoring for vulnerabilities with L&I defined standard configuration settings and any deviations, and implement controls to mitigate those vulnerabilities.

L&I OIT shall implement NIST Security Content Automation Protocols (SCAP) for security settings where feasible.
L&I OIT shall follow IRS Safeguards Computer Security Evaluation Matrix (SCSEM) controls and settings where feasible as well as document discrepancies from SCSEM and other compensating controls.
L&I OIT shall obtain a waiver from the L&I Enterprise Change Approval Board (ECAB) to deviate from these controls for configuration settings and document this deviation following the ITSM Change Management process.

E. Least Functionality
L&I OIT shall implement controls in accordance with the L&I SEC-010 Access Control policy including role based access, separation of duties, and least privilege.
L&I OIT shall document varying levels of access for each phase of the SDLC.
L&I OIT shall monitor for changes in role access following the L&I Incident Management plan.
L&I OIT shall obtain a waiver from the L&I ECAB to deviate from these controls for least functionality and document any deviation following the ITSM Change Management process.

F. Security Impact Analysis
L&I OIT shall establish a Security and Architectural Review (SAR) panel. The SAR panel shall conduct a security impact analysis of all changes, prior to a change being submitted to the ECAB. Change documentation shall indicate when the analysis was performed, who completed the analysis, the results of the analysis, risks, and the approval/disapproval information.

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-010 - Access Control policy

SYM-001 - Contingency Planning & Training Policy

SYM-003 – Configuration Settings Policy

IRS Publication 1075

7. Version Control:

Version	Date	Purpose
1.0	06/2016	Base Document
1.1	01/2017	Format and content revision
1.2	02/2017	Remove backup add new policy links