pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SYM-003

Name:	Configuration Settings
Effective Date:	March 2017
Category:	System Management
Version:	1.1

1. Purpose:

This policy provides direction and identify guidelines regarding configuration settings policies; fulfills the requirements of Internal Revenue Service (IRS) Publication 1075; and implements the safeguards and 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 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 settings. IRS Publication 1075 provides direction regarding acceptable configuration settings standards to help ensure that the agency is functioning consistently and at peak efficiency. The IRS Office of Safeguards defines the compliance requirements (e.g., Safeguard Computer Security Evaluation Matrices (SCSEMs) and assessment tools) for the secure handling of Federal Tax Information (FTI).

The authoritative source for platform checklists used by the Office of Safeguards is the NIST Checklist Program Repository (http://checklists.nist.gov). Office of Safeguards SCSEMs may include compliance requirements from one or more of the following security benchmarks:

- United States Government Configuration Baseline (USGCB)
- Center for Internet Security (CIS) Benchmarks
- Defense Information Systems Agency (DISA) Security Technical
- Implementation Guides (STIGS)
- National Security Agency (NSA) Configuration Guides

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 (hereinafter referred to collectively as "L&I Users").

4. Policy:

A. Configuration settings for FTI data:

L&I OIT shall establish and document configuration settings for all IT Equipment and systems that receive, process, store, or transmit FTI using the most restrictive modes consistent with the IT Equipment's operational requirements.

L&I OIT shall establish and document compensating controls where operational requirements deviate from the most restrictive modes.

L&I OIT shall implement the documented configuration settings on all IT Equipment and systems that receive, process, store, or transmit FTI.

L&I OIT shall monitor changes to the configuration settings in accordance with agency policies and procedures for configuration setting changes.

L&I OIT shall restrict changes following SYM-002 Configuration Management Policy.

B. Configuration settings for other Protected data:

L&I OIT shall establish and document configuration settings for all IT Equipment and systems that receive, process, store, or transmit sensitive data, per OA ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data using the restrictive modes consistent with operational requirements, OA policies, and NIST controls.

L&I OIT shall implement the documented configuration settings on all IT Equipment and systems that receive, process, store, or transmit sensitive data.

L&I OIT shall monitor changes to the configuration settings in accordance with agency policies and procedures of configuration setting changes.

L&I OIT shall restrict changes following SYM-002 Configuration Management Policy.

C. Configuration settings for lab and development systems:

IT Equipment and systems in a lab or development environment shall be implemented with restrictive configuration settings consistent with the correlating production system and the data classification received, processed, stored, or transmitted on that production system.

5. Responsibilities:

A. L&I User responsibilities:

- Comply with all L&I policies, management directives and laws;
- Adhere to all established configuration settings policies; and
- Report any violations of policies promptly to 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

SYM-002 Configuration Management Policy

OA ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data

OA ITP-SEC025 Proper Use and Disclosure of Personally Identifiable Information (PII)

IRS Publication 1075

7. Version Control:

Version	Date	Purpose
1.0	05/2016	Base Document
1.1	02/2017	Updates to content and formatting