pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy APP-001

Name:	Release of Protected Data Policy
Effective Date:	June 2017
Category:	Application
Version:	1.2

1. Purpose:

This policy facilitates information sharing by enabling authorized users to determine whether data may be shared based on the restrictions applied by the data owner. This policy establishes the minimum requirements for the Labor & Industry (L&I) Office of Information Technology (OIT) to protect sensitive data, 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 establishes controls to comply with Commonwealth executive order on open data. This policy is intended to meet the control requirements outlined in IRS Publication 1075, the National Institute of Standards and Technology (NIST) NIST critical controls: AC-3, 21, CM-8, IR-6, MP-6, PE-3, SA-9, SC-4, & SC-8 Per SP 800-53 R4.

2. Background:

L&I has data sharing agreements within the agency, with other state agencies and with federal agencies. In light of the Governor's executive order on open data, this policy will provide the framework including decision points where the business will determine what can and cannot be shared.

Information that is restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) requires controls to ensure the confidentiality, integrity, and availability of that data. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

Controls to share data are to reduce risk of data breach by releasing data inappropriately and add value by releasing valuable information that has been treated in accordance with applicable laws, statutes, and policies.

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. Business area

Business area staff shall assist OIT in the classification of all data types received, processed, or stored on their system. Classification shall include categories of data that can or cannot be released.

Business area staff, and system owners shall report sharing agreements and requirements of the Data Owner to OIT.

Business area staff shall document sharing agreements and requirements.

L&I shall not share data owned by a third party without express written consent from the data owner following their requirements, e.g. IRS Publication 1075.

Business area staff and OIT shall review all requests for the release of data following the Requesting Release of Protected Data Procedure.

B. OIT

OIT shall comply with data classification requirements of ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data. All project and system development efforts shall adhere to NIST Security Controls, based on data classification.

OIT shall develop controls to ensure sensitive data is protected for confidentiality, integrity, and availability.

OIT shall coordinate with business area staff and L&I management to determine data sharing requirements. OIT shall assist business area staff in making information sharing/collaboration decisions.

OIT shall coordinate with the business area and Office of Chief Counsel (OCC) to coordinate and document the sharing of data with other agencies. OIT shall review the agreement documents annually and consult with the business area and OCC as necessary.

OIT shall not use data in development environments that has not been redacted, hashed, or otherwise obfuscated to ensure data integrity.

OIT shall establish logging for audit purposes in compliance with OA ITP-PRV001, and NIST Security Controls.

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 the release of protected data.

6. References:

L&I Policy Definitions Document

Requesting Release of Protected Data

ADM-002 - ITIL Compliance

APP-000 – System Development Life Cycle

ITP-PRV001 - Commonwealth of Pennsylvania Electronic Information Privacy Policy

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

Executive Order 2016-07 - Open Data, Data Development, and Data Governance

IRS Publication 1075

NIST SP 800-53 R4

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base Document
1.1	08/2016	Format and Content Revision
1.2	06/2017	Integration of ITIL and SDLC policies