pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy Security SEC-001

Name:	Personally Identifiable Information Storage and Transfer
Effective Date:	July 2017
Category:	Security
Version:	1.2

1. Purpose:

This policy defines the data elements that are considered personally identifiable information (PII) for the PA Department of Labor & Industry (L&I). This policy will identify guidelines for the transfer and storage of PII by L&I.

This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-1, 21 & SC-4 Per SP 800-53 R4.

2. Background:

This policy is published under the general authority of the information technology policies (ITP)s published by the Office of Administration / Office of Information Technology (OA/OIT), in that it identifies key roles and responsibilities in support of ITPs.

While the Office of Information Technology (OIT) are the custodians of the data, the data owners determine the security controls that must be implemented on their data. System owners are responsible for ensuring their systems are compliant with statutes, regulations, and laws governing the receipt, processing, and storage of PII. Failure to correctly identify and protect PII could result in the loss of service, loss of state or federal funding, or place L&I at risk of legal and financial repercussions.

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:

OIT shall take all necessary steps to protect the PII of all L&I Users and constituents by minimizing or eliminating the use of PII. System owners (SO) shall determine if PII must be transmitted and stored.

The SO shall annually identify and classify data in the system to ensure all PII data is encrypted at rest and in transit. If data categorized as PII is not properly encrypted, a corrective action plan (CAP) must be created to address this vulnerability in a timely manner. The plan will be created by OIT and the application/system owner/administrator, and approved by the delivery center information security officer (ISO) and chief information officer (CIO) or deputy chief information officer (DCIO). Legacy systems will *not* be grandfathered in.

For the purposes of L&I, PII is any information that can be used to uniquely identify an individual's identity or information that is linkable to an individual. This includes:

- Name
  - Full name
  - Maiden name
  - Mother’s maiden name
  - Alias
- Date of Birth
- Personal identification numbers
  - Social Security number (SSN)
  - Passport number
  - Driver’s license number
  - State identification card number
  - Taxpayer identification number
  - Federal Employer Identification Number (FEIN) or Employer Identification Number (EIN)
    - In cases where SSN could be used as FEIN or EIN.
- Financial account or credit card numbers
- Address information
  - Street address
  - Mailing address
  - Physical address
- Personal characteristics
  - Fingerprints
  - Biometric data (e.g., retina scan, voice signature, facial geometry)

If PII must be collected based on business requirements, it must be encrypted at rest and in transit in accordance with ITP-SEC020 and ITP-SEC031. This applies to the storage of PII on all devices and systems including servers, databases, application files, workstations/laptops, removable media, and network drives. Unless there is an approved detailed business requirement, PII may not be stored on a workstation, laptop, or removable media device. All exception business cases must be approved by the agency ISO and CIO/DCIO.

All PII or protected data within a database, shall be encrypted at the data level via the application. If this is not feasible, the entire database shall be encrypted. Any individual elements that constitute PII are protected data and must be secured per ITP-SEC019;. If

PII or protected data is stored on separate tables of the same database or separate databases and there is a key field or identifier that links the data; it must be encrypted.

All PII data elements must be encrypted with at least a 256-bit encryption algorithm. This applies to all means of electronic transmission of PII including; e-mail, web-based applications, web-based forms, fax, file transfer protocol (FTP), and server/on-line document sharing and storage systems.

A data breach is defined by the Breach of Personal Information Notification Act. If a breach is declared, L&I will follow all required OA, state, and federal laws and mandates related to remediation and notification to the public.

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 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 securing PII.

6. References:

L&I Policy Definitions Document

ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data

ITP-SEC020 Encryption Standards for Data at Rest

ITP-SEC024 IT Security Incident Reporting Policy

ITP-SEC025 Proper Use and Disclosure of Personally Identifiable Information

ITP-SEC031 Encryption Standards for Data in Transit

Breach of Personal Information Notification Act, December 22, 2005, P.L. 474, No. 94

NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

7. Version control:

Version:	**Date:**	**Purpose:**
0.1	04/2014	Initial draft created
1.0	07/2014	Published
1.1	07/2016	Updated to include approvals and new content
1.2	07/2017	Annual review & content revision