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 2016
Category:	Security Domain
Version:	1.1

1. Purpose:

The purpose of this policy is to define the data elements that are considered Personally Identifiable Information (PII) for the PA Department of Labor & Industry (L&I). This policy also covers how PII must be transferred and stored by L&I.

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.

This policy ensures L&I is identifying and protecting all PII in accordance with applicable state and federal laws and mandates, and Office of Administration (OA) policy. 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.

4. Policy:

It is the intent of the Office of Information Technology (OIT) to take all necessary steps to protect the PII of all of L&I employees, users, and constituents by minimizing or eliminating the use of PII. This policy will identify and define data elements that are considered PII. If it is determined that PII must be transmitted and stored, this policy defines the minimum requirements for transmitting and storing PII.

Identification and classification of PII should be done by the system owner at least yearly, to ensure all PII data is encrypted at rest and in transit. If it is identified that 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 Enterprise Security and Compliance (ESC) section and the application/system owner/administrator, and approved by the L&I Chief Information Security Officer (CISO) 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 OA ITP-SEC020 and OA ITP-SEC031. This applies to the storage of PII on all devices and/or systems including servers, databases, application files, workstations/laptops, removable media, and network drives. Unless there is a detailed business requirement, PII should never be stored on a workstation, laptop, or removable media device. These business cases must be approved by the agency CISO and CIO/DCIO.

When storing PII within a database, encryption should occur at the data level via the application. If this is not feasible, the entire database should be encrypted. Individual elements are sensitive data per OA ITP-SEC019, however, any two or more elements constitute PII and must be encrypted. If PII 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 constitutes PII and the database(s) 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 PII 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:

Violations of the department's policies may result in disciplinary action up to and including termination of employment or contractor sanctions.

A. Employee Responsibilities:

- Identify and properly secure all PII in accordance with this policy.
- Complete the mandatory security awareness training.
- Comply with all security policies, management directives, and laws.

B. L&I Management Responsibilities:

- Understand the effects of data compromise.
- Follow this policy to protect PII.
- Ensure employees comply with all L&I policies.

6. References:

L&I Policy Definitions Document

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

OA ITP-SEC020 Encryption Standards for Data at Rest

OA ITP-SEC024 IT Security Incident Reporting Policy

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

OA ITP-SEC031 Encryption Standards for Data in Transit

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

NIST, 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