pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Procedure

Name:	Reporting Information Security Incidents
Effective Date:	December 2016
Category:	Security
Version:	1.1

1. Scope:

This procedure applies to all Department of Labor & Industry (L&I) employees and business partners, and contractors when L&I has declared or suspects a breach or loss of Personally Identifiable Information (PII) or a security incident, which includes Social Security Administration (SSA) Internal Revenue Service (IRS) provided data such as Federal Tax Information (FTI).

2. Procedure:

The procedure is implemented by various IT staff under the direction of the L&I Chief Information Security Officer (CISO) under the authority of the Chief Information Officer (CIO), or Deputy Chief Information Officer (DCIO).

Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents by any commonwealth employee, or any other person, the individual making the observation or receiving information

Step	**Responsibility**	**Action**
1.	Individual who identified the incident	Immediately report the details of the incident to their supervisor. If unavailable, the reporting individual should immediately complete step 2 below: If appropriate, contact the proper authorities for any workplace violence* event (e.g., theft of equipment). *The HR reporting form would also be required for such an incident per: Bureau of Human Resources' Information Bulletin 2007-06
2.	Supervisor/Reporting Individual	Within one (1) hour, complete the Security Incident Reporting form for L&I with as much detail as possible. E-mail the completed form to L&I CISO RA-LI-OIT-DLICISO@pa.gov
3.	CISO	Notify the agency CIO, Communications and Press Office (CPO) and Deputy Secretary for Administration immediately after confirmation that a High or Critical level information security incident has occurred and an L&I incident tracking number has been assigned.

4.	CISO	In coordination with appropriate OIT staff, isolate affected IT equipment, remove stolen assets access to the network (work with reported agency for stolen devices), and check for any compromised data or propagation of the problem.
5.	CISO	Complete the IT Security Incident Online Reporting form. If necessary, organize a Security response team through the Commonwealth CISO.
6.	CISO	If required, works with the program area and CPO on notification process for any potential breach of critical data. This is to be coordinated only after the full extent of the incident has been identified.
7.	CISO	If FTI data is involved, the procedures outlined in Security Incident Reporting for Internal Revenue Service
8.	CISO	If SSA data is involved then the procedures in Security Incident Reporting for Social Security Administration

3. References:

L&I, OIT Policy Definitions

SEC-008 – Security Incident Response Policy

Security Incident Reporting for Social Security Administration

Security Incident Reporting for Internal Revenue Service

Security Breach Checklist

OA ITP-SEC024 IT Security Incident Reporting Policy

4. Version Control:

Version	Date	Purpose
1.0	01/2006	Base Document
1.1	12/2016	Merged documents, formatted, revised content