pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-008

Name:	Security Incident Response Policy
Effective Date:	December 2016
Category:	Security
Version:	1.1

1. Purpose:

To establish standard practices and response plans regarding Department of Labor & Industry (L&I) Information Technology (IT) Equipment and/or data during an IT Information Security Incident or Cyber Security Incident (hereinafter "Security Incident") while fulfilling the requirements of the Internal Revenue Service (IRS) Publication 1075, and OA ITP SEC024. This policy will be a roadmap for implementing L&I's Security Incident response capabilities including incidents categorized as a data breach.

This policy provides examples of incidents that are considered security incidents, establishes the organizational structure for Security Incident response, defines roles and responsibilities, and lists the requirements for reporting a Security Incident, among other items.

This policy defines further actions to be taken when the confidentiality, integrity, or availability of Federal Tax Information (FTI) data or Social Security Administration (SSA) data may have been compromised.

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, which identifies key roles and responsibilities regarding a Security Incident response plan. IRS Publication 1075 provides direction regarding acceptable Security Incident response plan standards to help ensure that L&I is prepared and equipped to handle future events or Security Incident.

Information Security & Cyber Security Incidents examples include:

- Theft or loss of any commonwealth IT equipment, including but not limited to: (laptop, desktop, cellphone/smartphone, memory sticks, USB drives);
- Suspected or actual break-in of a commonwealth or L&I computer or network;
- L&I website defacements or compromises;
- Detection of malicious code on an individual's workstation/electronic device;
- Connection of non-commonwealth computers and servers to the L&I network without authorization or in violation of security policies;
- Attempts to circumvent access to any L&I blocked websites;
- Attempts to gain unauthorized access to a system or its data;
- Unauthorized changes to system hardware, firmware, or software;
- Misuse of government property, facilities, or services, including accepting payment or services to provide access to, or use of, L&I IT resources;

- Use of L&I IT resources in excess of one's authority;
- Storage and/or distribution of child pornography;
- Denial of service (DoS) attacks against L&I information systems;
- Unauthorized use of a system for the transmission, processing, or storage of data;
- Loss and/or theft of department files containing confidential citizen data;
- Loss and/or theft of business documentation and or guides that contain non-public data.

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:

L&I OIT will follow a Security Incident management process plan. The first goal of the Security Incident management process plan is to ensure the security of L&I's data, followed by service restoration. There are four phases to security incident response:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity

L&I will leverage all existing systems and staff to monitor for a Security Incident, restore IT services and resolve the Security Incident as quickly as possible with the least disruption to L&I's business, while protecting L&I data and systems.

L&I OIT will develop and maintain controls over IT systems to reduce risk in a defense in depth strategy. L&I OIT will collect and correlate event information from IT Systems, endpoint security tools, and Intrusion Detection Systems (IDS) to determine if a Security Incident has occurred.

L&I Users shall immediately report the discovery of a Security Incident and/or when suspicious computer-related activities are detected on L&I Systems. L&I Users shall complete and submit the L&I Information Security Incident Reporting Form within one (1) hour of to L&I's Chief Information Security Officer (CISO) RA-LI-OIT-DLICISO@pa.gov, in accordance with L&I Security Incident Management Procedure.

L&I OIT staff shall promptly investigate all Security Incidents as directed by the L&I CISO, or Chief Information Officer (CIO) / Deputy Chief Information Officer (DCIO).

The L&I CISO shall categorize all Security Incidents using the Security Breach Checklist and OA ITP-SEC024, and report as required, to:

- The OA provided Enterprise Governance, Risk, and Compliance (eGRC) tool

- United States Computer Emergency Readiness Team (US-CERT), for SSA Security Incident
- Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), for FTI Security Incident

The L&I CISO shall appoint a Security Incident Response Team (SIRT) as necessary. The SIRT shall promptly and correctly handle a Security Incident so that it can be quickly contained, investigated, and recovered from. SIRTs will consist of any or all of the following: management from the affected business area, OIT management, the L&I CISO, the L&I OIT Problem/Incident Manager, Subject Matter Experts (SMEs) for affected systems, internal auditors, L&I Office of Chief Counsel (OCC), L&I Bureau of Human Resources (HR), L&I Communications and Press Office (CPO). The SIRT will work with management from the business area including, as necessary, executive staff to determine if a Disaster Recovery (DR) plan should be invoked.

L&I OIT System Administrators (SA), including operations staff, shall advise and assist the L&I CISO in the assessment and containment actions, as necessary. The SIRT may invoke different countermeasures as part of the immediate response to a Security Incident, depending on the type and severity of the incident, the value of the affected assets, and risk of greater impact.

The L&I CISO may invoke other activities to mitigate risk of further exposure such as:

- Information gathering - enabling verbose logging, backups, system snapshots and updated event monitors.
- Configuration changes –hardware reconfiguration, and, Operating System (OS) or application patches.
- Forensics – collection of digital data for root cause analysis, to prevent spread of infection, or for law enforcement.
- Isolation – moving the affected IT resource to a separate network.

The program area shall be engaged by the L&I CISO or CIO/DCIO to declare an outage or invoke their Disaster Recovery plan.

The L&I CIO has the final authority on all decisions relating to the management of or response to a major Security Incident. The L&I CIO shall notify the L&I Secretary and the L&I CPO of all major Security Incidents and provide regular updates as necessary.

L&I management shall leverage their respective staff to support a SIRT and maintain workloads.

The following procedures will be used in all Security Incident:

Procedure Name	When Used	Reporting Window	Prepared by	Submit to
Security Breach Checklist Procedure	Any Security Incident	1 hour	L&I CISO	OA eGRC
Reporting Information Security Incidents Procedure	During a declared or suspected breach or loss of PII	1 hour	L&I CISO	OA eGRC
Security Incident Reporting for Internal Revenue Service Procedure	When FTI is involved	24 hours	Any L&I staff OR L&I CISO	IRS Special Agent-in-Charge TIGTA
Security Incident Reporting for Social Security Administration Procedure	When SSA data is involved	1 hour	Any L&I staff OR L&I CISO	US-CERT

The L&I CISO shall maintain policies and procedures for L&I's compliance with IRS/ and SSA requirements, state statutes, business objectives, and policies. In the event of a Security Incident, the L&I CISO, in conjunction with OIT staff and the L&I CIO/DCIO, shall evaluate all Security Incident according to the IT Security Incident Reporting Procedures in OA ITP-SEC024.

The SIRT shall continue to meet during recovery operations and beyond to conduct post-incident activities, as necessary.

5. Responsibilities:

A. L&I User responsibilities:

- Report immediately all suspicious computer-related activities detected on L&I Systems to the supervisor, and appropriate OIT staff as defined in the L&I Security Incident Procedure;
- Report alerts and warnings from agency endpoint security tools;
- Report all lost or stolen equipment per SEC-003;
- Complete and submit the L&I Information Security Incident Reporting Form immediately when the discovery of the information Security Incident and/or when suspicious computer related activities are detected on L&I Systems;

- Adhere to this policy and related procedures and any other agency security policies and procedures; and
- Fully cooperate with any subsequent OIT investigation.

B. L&I management responsibilities:

- Communicate policy and procedures to all employees;
- Ensure all employees complete all mandatory information security awareness training;
- Implement procedures to ensure compliance with the initial notification procedures described in this policy;
- Reassign work as necessary until the Security Incident is resolved; and
- Ensure employees comply with all L&I policies.

6. References:

L&I Policy Definitions Document

Security Breach Procedure

Reporting Information Security Incidents Procedure

Security Incident Reporting for Social Security Administration

Security Incident Reporting for Internal Revenue Service

SEC-003 Lost or Stolen Equipment

OA ITP-SEC024 IT Security Incident Reporting Policy

IRS Publication 1075

7. Version Control:

Version	Date	Purpose
1.0	08/2008	Base Document
1.1	12/2016	Reformatted, revised content