

L&I, Office of Information Technology Procedure

| | |
|------------------------|--|
| Name: | Security Incident Reporting for Internal Revenue Service |
| Effective Date: | August 2018 |
| Category: | Security |
| Version: | 1.2 |

1. Scope:

This procedure applies to all Department of Labor & Industry (L&I) employees, business partners, and contractors when L&I has declared or suspects a breach or loss of Personally Identifiable Information (PII) or a security incident that includes 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 can also contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA).

| <u>Step</u> | <u>Responsibility</u> | <u>Action</u> |
|-------------|-----------------------|--|
| 1. | 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. |
| 2. | CISO | Coordinate incident with L&I and Office of Administration (OA) Enterprise Security. |
| 3. | CISO | Notify the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident. |
| 4. | CISO /Any employee | <ul style="list-style-type: none"> • Contact the appropriate Special Agent-in-Charge TIGTA, within 24 hours. • Email the Office of Safeguards: safeguardreports@irs.gov |

If the TIGTA or Office of Safeguards is notified first, the employee must notify the CISO immediately afterward.

L&I, Office of Information Technology Procedure

5. CISO Provide updates as they become available to IRS contact and Office of Safeguards, as appropriate.

Contact information for TIGTA resources:

| Field Division | States Served by Field Division | Telephone Number |
|-----------------------|--|-------------------------|
| Washington | Delaware, Maryland, New Jersey, Pennsylvania, Virginia, Washington DC, West Virginia | (215) 861-1003 |

3. References:

[L&I, OIT Policy Definitions](#)

[SEC-008](#) – Security Incident Response Policy

[Reporting Information Security Incidents](#)

[Security Incident Reporting for Social Security Administration](#)

[Security Breach Checklist](#)

[OA ITP-SEC024](#) IT Security Incident Reporting Policy

4. Version Control:

| <u>Version</u> | <u>Date</u> | <u>Purpose</u> |
|-----------------------|--------------------|--|
| 1.0 | 08/2008 | Base Document |
| 1.1 | 12/2016 | Reformatted, revised content |
| 1.2 | 08/2018 | Added contact information for Office of Safeguards for CAP |