

**L&I, Office of Information Technology Policy SEC-009**

|                        |  |
|------------------------|--|
| <b>Name:</b>           | Federal Tax Information Data Compliance Policy |
| <b>Effective Date:</b> | September 2017                                 |
| <b>Category:</b>       | Security                                       |
| <b>Version:</b>        | 1.3  |

**1. Purpose:**

This policy identifies guidelines for the proper handling of Internal Revenue Service (IRS) data per IRS [Publication 1075](#) and [NIST SP 800-53](#), which provide handling and storage guidance for federal tax information (FTI). This policy identifies guidelines to protect sensitive information, including FTI, from unauthorized access and improper disclosure in compliance with safeguards and requirements defined by the Social Security Administration (SSA) and the IRS. This policy documents the implementation of the National Institute of Standards and Technology ([NIST Security Controls](#): SC-19 Per [SP 800-53 R4](#)).

**2. Background:**

The Department of Labor & Industry (L&I) Office of Information Technology (OIT) is required to enact policy and procedure to ensure the confidentiality, integrity, and availability of FTI data. L&I offices, bureaus, and divisions are required to comply with IRS [Publication 1075](#) when FTI is stored and transmitted through L&I systems. L&I will follow safeguards required by the IRS for the protection of FTI as prescribed in the aforementioned IRS publication.

**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 will conduct background checks for all L&I employees who handle FTI in accordance with IRS Pub 1075.

L&I will maintain documentation of annual training of all L&I Users' completion of Security Awareness Training and Federal Tax Information Training, according to IRS FTI guidance, for L&I Users whose responsibilities and jobs entail utilizing and processing FTI data (IRS 1075 Section 6.2).

All L&I Users shall report all incidents or suspected incidents relating to FTI data as outlined in [SEC-008](#) Incident Response Reporting (IRS 1075 Section 9.3.8).

All L&I Users shall strictly limit access to FTI data to only those individuals whose jobs require such access (IRS 1075 Sections 5.2.1 and 7.2).

All L&I Users shall ensure that FTI data remains physically secured and under strict control at all times (IRS 1075 Section 4.2 and 9.3).

## **L&I, Office of Information Technology Policy SEC-009**

L&I Users may not discuss FTI over the phone (IRS 1075 Section 9.4.5 & 9.4.15). All L&I Users shall ensure that FTI is not discussed over the phone.

L&I OIT will ensure that all L&I Users who have remote access to FTI over the Internet use two-factor authentication (IRS 1075 Section 9.3).

L&I OIT will document existing interfaces that handle FTI and ensure that no new interfaces to FTI are created or modified (IRS 1075 Section 9.3).

L&I management and OIT staff shall regularly update the system security plan, security administrator guides, and security user guides. Additionally, they will follow rules of behavior for systems containing FTI (IRS 1075 Section 9.3.12).

L&I management and OIT staff shall certify, in writing, that the security controls in systems containing FTI are adequately implemented to protect FTI (IRS 1075 Exhibit 10).

L&I program areas that handle FTI shall create documented procedures implementing security controls in compliance with Pub 1075 for protecting FTI sent or received via fax transmission, or shall certify, in writing to the information security officer (ISO), that they do not send or receive FTI via fax.

All L&I Users shall encrypt any FTI transmitted via e-mail (IRS 1075 Section 9.4).

L&I OIT will maintain overall system and data integrity of FTI data as documented in the system security plans (IRS 1075 Section 9.3.12)..

### **5. Responsibilities:**

A. L&I User responsibilities:

- Comply with applicable established OIT security policies and procedures; and
- Report possible or suspected improper inspection or disclosure of FTI to the ISO.

B. L&I management responsibilities:

- Comply with all L&I policies and procedures and ensure L&I Users comply with all L&I policies and procedures;
- Ensure L&I Users complete the mandatory Cyber Security Awareness training; and
- Ensure L&I Users who handle FTI complete the Federal Tax Information training; and
- Adhere to this policy and any published procedures regarding FTI compliance.

### **6. References:**

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

[Federal Tax Information Fax Handling for UC Benefits Procedure](#)

**L&I, Office of Information Technology Policy SEC-009**

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

[Security Breach Procedure](#)

[Security Incident Reporting for Internal Revenue Service](#)

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

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

[IRS Publication 1075](#)

[NIST Special Publications](#)

**7. Version Control:**

| <b><u>Version</u></b> | <b><u>Date</u></b> | <b><u>Purpose</u></b>           |
|-----------------------|--------------------|---------------------------------|
| 1.0                   | 02/2013            | Base Document                   |
| 1.1                   | 09/2014            | Update to new policy format     |
| 1.2                   | 12/2016            | Format and Content Revision     |
| 1.3                   | 09/2017            | Update for voice communications |