pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

**L&I, Office of Information Technology Policy PLT-004**

| | |
|---|---|
| **Name:** | Inventory of Authorized & Unauthorized Hardware & Software |
| **Effective Date:** | March 2017 |
| **Category:** | Platform Domain |
| **Version:** | 1.1 |

## 1. Purpose:

This policy manages accountability regarding licenses, hardware, and software at the Department of Labor & Industry (L&I). This policy establishes controls to reduce the ability of attackers to find and exploit unauthorized and unprotected systems. This policy provides direction for the use of active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices. This policy identifies guidelines for identifying vulnerable or malicious software to mitigate or root out attacks. This policy requires the creation of a list of authorized software for each type of system, the deployment of tools to track software installed (including type, version, and patches), and monitoring for unauthorized or unnecessary software.

## 2. Background:

This policy is published under the general authority of the Governor's Office of Administration / Office of Information Technology (OA/OIT). L&I uses an itemized asset inventory list of hardware and software, as well as an Information Technology Service Management (ITSM) tool to help manage and maintain data of its physical devices and software. L&I's ITSM tool stores inventory data in a Configuration Management Database (CMDB).

A current and updated inventory of authorized and unauthorized hardware and software is a critical security control and touches on these NIST Special Publication 800-53 (Rev. 4) security controls: CA-7, CM-2, CM-8, CM-10, CM-11, IA-3, PM-5, SA-4, SC-34, & SI-4. Additionally, this inventory will aid L&I in implementing the top five controls from the Center for Internet Security (CIS), which are internationally recognized, developed, refined, and validated controls.

## 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 shall develop and maintain a system to inventory data from all IT Equipment, systems, and software connected to the L&I network and the network devices themselves. L&I OIT shall manage the system by establishing system change controls, permissions, guidelines, and procedures.

For each Configuration Item (CI) the CMDB shall record at least these items:

- display name
- host name
- serial number
- asset tag
- network addresses
- MAC address
- status
- location code
- department
- operating system
- related systems
- System Owner
- asset owner
- related users
- departmental unit

The L&I ITSM CMDB shall be the only authorized repository of this inventory.

L&I OIT shall update the CMDB as part of normal change control processes.

L&I OIT shall develop and document procedures to update each physical CI with an asset tag as part of the deployment and disposal processes, in accordance with PLT-002.

L&I OIT shall secure the ITSM CMDB and provide role based access limited to authorized OIT staff to update the ITSM CMDB as part of normal change control processes. All access to ITSM CMDB and changes to the ITSM CMDB will be logged and are auditable events.

L&I OIT shall ensure the CMDB distinguishes IT equipment by categorization. Portable electronic devices that store or process L&I data, including but not limited to, mobile phones, tablets, and laptops, must be recorded in the CMDB regardless of whether they are attached to the L&I's network. External storage devices procured by L&I must also be recorded in the CMDB.

L&I OIT shall identify and categorize IT equipment and systems according to the Mission Critical Application (MCA) list and the "VIP" status of the user, as defined by the ITSM tool.

L&I OIT shall deploy software inventory tools to create a baseline inventory for each of the operating system types and major revisions in use at L&I, including servers, workstations, and mobile devices. Each successive approved Operating System (OS) version will require a new baseline inventory of hardware and software, per L&I SYM-002 Configuration Management Policy.

L&I OIT shall restrict access to all inventory tools and shall monitor for unauthorized use of passive or active scanning tools.

L&I OIT shall develop a list of authorized software that is required for each type of system including servers, workstations, and portable devices.

L&I OIT shall develop procedures and controls that allow systems to run only approved software while preventing the execution of all other software. The addition or removal of a white listed application shall follow L&I OIT Change Management procedures.

L&I OIT shall establish monitoring which shall produce incidents in the ITSM tool following L&I's Incident Response plan. When the ITSM tool discovers deviations, it will generate and send reports to the L&I Chief Information Security Officer (CISO).

L&I OIT shall ensure that the ITSM CMDB is up to date by reviewing reported deviations from the expected inventory of IT equipment on the network. Continuous monitoring for the installation of unauthorized software shall be enabled on all devices connected to the L&I network. Unauthorized software includes legitimate system administration software installed on systems where there is no business need for it.

L&I OIT shall develop procedures for the identification and removal of unauthorized software.

L&I OIT shall conduct annual audits of the ITSM CMDB system data for additions and changes.

**5. Responsibilities:**

A. L&I User responsibilities:

- Comply with all established OIT policies;
- Report possible or suspected unauthorized use of IT equipment to the L&I CISO at LI, OIT-DLICISO; and
- Report possible or suspected unauthorized software to the L&I CISO at LI, OIT-DLICISO.

B. L&I management responsibilities:

- Ensure that users comply with all established OIT policies; and
- Follow this policy and any supporting procedures.

**6. References:**

L&I Policy Definitions Document

PLT-002-Disposition of IT Equipment and Electronic Waste Products

SYM-002-Configuration Management Policy

SYM-003-Configuration Settings Policy

**7. Version Control:**

| Version | Date | Purpose |
|---|---|---|

**L&I, Office of Information Technology Policy PLT-004**

| | | |
|---|---|---|
| 1.0 | 02/2007 | Base Document |
| 1.1 | 03/2017 | Format and Content Revision |