pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-014

Name:	Information Technology Equipment Restrictions
Effective Date:	August 2017
Category:	Security
Version:	1.1

1. Purpose:

This policy identifies guidelines for the use of peripheral devices with Commonwealth provided IT Equipment, conducting Commonwealth business remotely, and utilization of removable storage for all Department of Labor & Industry (L&I) users.

This policy establishes controls for the storage of sensitive data, including Personally Identifiable Information (PII), on Commonwealth IT Equipment. This policy documents the protection of sensitive information, including Federal Tax Information (FTI), from unauthorized access and improper disclosure in compliance with safeguards and requirements defined by the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-19, MP-2, MP-3, MP-4, MP-5, MP-6, SI-1 and SI-3 Per SP 800-53 R4.

2. Background:

L&I IT Equipment is consistently maintained with security safeguards and protections to ensure the highest posture of confidentiality, integrity, and availability of the information that L&I handles daily.

The introduction of non-Commonwealth IT Equipment into or onto the L&I network by any means provides the potential for systems to be compromised.

Violations of L&I's policies may result in disciplinary action up to and including termination of employment or contractor sanctions (including loss of e-mail, Internet, or computer access privileges).

3. Scope:

This policy applies to all employees within all bureaus, divisions, boards, commissions, and councils within L&I. This includes any contracted employees in the service of L&I. (hereinafter referred to collectively as "L&I Users")

4. Policy:

A. Restrictions

L&I Users of Commonwealth provided IT Equipment shall not connect any non-Commonwealth provided devices or peripherals to the Commonwealth Network without prior approvals from their management and the Information Security Officer (ISO). This includes all non-Commonwealth IT Equipment (vendor, personal, or

otherwise); networking equipment, including wireless access points; network storage devices; and printers.

L&I Users of the Commonwealth network shall not directly connect any non-Commonwealth IT equipment to the L&I infrastructure without prior approvals from their management and the Information Security Officer (ISO).

L&I Users who connect remotely shall only conduct Commonwealth business via the Commonwealth provided remote access solution using the Virtual Private Network (VPN). All Commonwealth business must be conducted via a secured connection.

L&I Users shall report the loss or theft of all IT Equipment per SEC-003 and SEC-008.

L&I Users shall not connect non-Commonwealth mobile devices to Commonwealth provided IT Equipment for the purpose of charging the device.

L&I Users shall not store Citizen or business entity data on removable/mobile media such as:

- Personally Identifiable Information (PII) (e.g. Social Security Numbers);
- Financial Data,
  - Including Credit/Debit card information;
- Health Insurance Portability and Accountability Act (HIPAA) data,
  - Medical data directly associated with any individual;
- Federal Employer Identification Number (FEIN),
  - Tax ID's and other uniquely identifiable business information reported to the Department; and
- Passwords, account PINS, security codes or any other uniquely identifiable information.

OIT shall restrict access to miscellaneous media/devices with self-executing programs and shall monitor the use of removable storage media.

B. Proper Usage

L&I Users shall obtain approval from the ISO for new procurements of removable storage devices.

L&I Users shall only use Commonwealth provided and approved removable media devices including USB thumb drives, CD's/DVD's, digital cameras, digital recorders, and iPhones.

L&I Users shall ensure that the appropriate safeguards are implemented for sensitive data being stored.

OIT shall monitor the use of peripherals and storage of protected or PII data on removable/mobile media.

5. Responsibilities:

A. L&I User responsibilities:
   - Comply with all L&I policies, management directives, and laws; and
   - Report any violations of policies promptly to the L&I Information Security Officer at LI, OIT-DLICISO.

B. L&I management responsibilities:
   - Comply with all L&I policies and ensure L&I users comply with the policies; and
   - Obtain ISO approval for new procurements of removable storage; and
   - Adhere to this policy and any published procedures regarding IT equipment usage.

6. References:

L&I Policy Definitions Document

APP-001 - Release of Protected Data

NET-001 - Mobile Device Usage

SEC-001 - Personally Identifiable Information Storage and Transfer

SEC-004 - Computer and Information Security

SEC-008 - Security Incident Response

SEC-011 - Remote Access to the Commonwealth Network

ITP-PLT012 - Use of Privately Owned PCs to Access CoPA Resources

ITP-SEC020 - Encryption Standards for Data at Rest

ITP-SEC035 - Mobile Device Security Policy

MD 205.34 - Commonwealth of Pennsylvania Information Technology Acceptable Use Policy

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base Document
1.1	08/2017	Format and Content Revision