pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-003

Name:	Lost or Stolen Equipment
Effective Date:	October 2017
Category:	Security
Version:	1.2

1. Purpose:

This policy defines what Department of Labor & Industry (L&I) employees are required to do when their assigned Information Technology (IT) equipment is lost or stolen. This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AT-2, IR-1, IR-4, IR-6 Per SP 800-53 R4.

2. Background:

This policy is published under the general authority of the information technology policies (ITPs) published by the Governor's Office of Administration, Office for Information Technology (OA/OIT), in that it identifies key roles and responsibilities in support of ITPs.

This policy identifies actions that L&I employees must complete when their assigned IT Equipment is lost or stolen. Lost or stolen IT equipment could result in a data breach or loss of service. That is, if the lost or stolen IT equipment contains sensitive or personally identifiable information (PII) a data breach may be declared pursuant to commonwealth law. Reporting lost or stolen equipment is mandated by Management Directive 205.34, and is part of the mandatory annual security awareness training.

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:

IT Equipment must be stored in a secure location whenever it is not in use.

L&I Users must not leave IT equipment in a non-secure location, such as an unattended vehicle, for an extended period of time or overnight.

L&I Users shall take the following actions if IT equipment is lost or stolen:

- File a police report with local law enforcement, if the L&I User suspects the IT equipment was stolen.
- Report the loss to his or her direct supervisor immediately upon discovery or at the start of the L&I User's next scheduled shift.
- Report the loss and submit a completed Lost or Stolen IT Equipment Checklist and Questionnaire to the Office of Information Technology (OIT) Enterprise Security and Compliance Section (ESC) resource account LI, OIT-Security (ra-lioit-security@pa.gov) immediately upon discovery or at the start of the L&I User's next scheduled shift.

OIT shall review the completed checklist, ask follow-up questions, determine next steps, and notify executive staff, the Office of Chief Counsel, and OA, as appropriate.

OIT shall follow ITP-SEC024 in response to a report of lost or stolen IT Equipment.

If the IT Equipment was not encrypted, OIT shall follow SEC-008 and related procedures in response to a declared data breach.

OIT shall follow PLT-004 regarding inventory of IT equipment.

OIT shall implement steps to protect L&I data such as locking an L&I User account, or remotely wiping data from a lost or stolen piece of IT equipment.

OIT shall develop additional controls and assess existing controls for containment, and recovery of data from IT equipment.

Failure to follow this policy may result in disciplinary action up to and including termination of employment or contractor sanctions.

5. Responsibilities:

A. L&I User responsibilities:

- Protect and secure assigned IT equipment;
- Report all lost or stolen IT equipment immediately upon discovery or at the start of their next scheduled shift;
- Complete and submit the Lost or Stolen IT Equipment Checklist and Questionnaire immediately upon discovery or at the start of their next scheduled shift;
- File a police report (if equipment is stolen);
- 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
- Adhere to this policy and any published procedures regarding lost or stolen IT Equipment.

6. References:

L&I Policy Definitions Document

Lost or Stolen IT Equipment Checklist and Questionnaire

PLT-004 - Inventory of Authorized & Unauthorized Hardware & Software

SEC-001 - Personally Identifiable Information Storage and Transfer

SEC-008 - Security Incident Response Policy

ITP-SEC024 - IT Security Incident Reporting Policy

MD 205.34 Commonwealth of Pennsylvania Information Technology Acceptable Use Policy

NIST Special Publications

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base document
1.1	08/2016	Format and content revision
1.2	09/2017	Annual review & content revision