pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-006

Name:	OIT Secured Area Access and Physical Security
Effective Date:	July 2017
Category:	Security
Version:	2.2

1. Purpose:

This policy establishes appropriate measures to safeguard the physical perimeter of the Department of Labor & Industry's (L&I) Office of Information Technology (OIT) workspaces. This policy provides direction for the security of L&I facilities that house information systems. This policy assists in compliance with all federal and state laws, including but not limited to the Internal Revenue Service (IRS) and Social Security Administration (SSA) security protocols; establishes acceptable standards for admittance to OIT secured areas, including data closets, computer rooms, L&I data centers, OIT storage areas, and OIT workspaces within all L&I and commonwealth facilities; and provides OIT employees and contractors with direction on the proper use and responsibilities associated with access to OIT secured areas. This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC, PE-1, PE-2, PE-3, PE-6, PE-7, and PE-8 Per SP 800-53 R4.

2. Background:

Agencies are required to develop physical security policies that ensure the security and availability of agency documents and information (reference Office of Administration(OA) policy ITP SEC029, Minimum Standards for Improving Physical Security Access). OIT secured areas contain vast amounts of expensive computer equipment and storage for critical and sensitive data, which require protection from unauthorized access, use, disclosure, modification, or destruction.

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:

Entrances to OIT secured areas will be safeguarded with key locks or controlled by the OIT Keycard Access System (KAS) utilizing the commonwealth photo ID access badges (ID badge) supplied to authorized individuals by the Department of General Services.

No one is allowed access to secured areas without first having their identification and privileges verified. A person is designated a visitor if they do not have a valid ID badge, or if their ID badge does not grant them access to the secured space.

L&I Users shall not store non-IT equipment in wiring closets. All wiring closet doors are to remain closed and secured. Remote sites with server cabinets must always be locked. OIT shall maintain control of all keys for all server cabinets. L&I Users shall not access any wiring closet without obtaining OIT approval first.

OIT shall ensure procedures and safeguards are in place, through both access controls and alarm detection, to identify and prevent unauthorized access of, or damage to, secured facilities that house L&I systems.

OIT will ensure visitors to secured areas, restricted workspaces, and data centers are documented in accordance with all state and federal requirements, including but not limited to the IRS and SSA requirements.

All visitors shall be escorted by an authorized individual at all times in secured areas. The act of tailgating/piggybacking, (use of the ID badge to open a secured door for anyone other than the cardholder) is forbidden.

A. Secured Areas:

OIT shall manage access to secured areas using the KAS. OIT shall provide access to secured areas, provide information to assist security management, monitor specific alerts, and report abnormal conditions to the agency Information Security Officer (ISO).

B. Accessing Restricted OIT Workspace:

All individuals within the confines of a restricted OIT workspace shall wear and display either their ID badge or a visitor's badge.

At the L&I central office located at 651 Boas Street, all visitors shall complete the security access log for the third floor OIT workspaces.

Any person granting access to the OIT restricted workspace shall ensure that the visitor completes the security access log for the area.

All visitors shall be escorted by an authorized individual at all times.

C. Accessing OIT Data Centers:

All individuals within the confines of the OIT data center shall display either their ID badge or visitor's badge.

All visitors shall be logged in the visitor's log, display their visitor's badge, and be escorted by a staff member with a valid ID badge.

Any L&I User who accesses the OIT data centers without an authorized ID badge shall complete the security access log for that secured area.

The L&I User granting access to the OIT data center shall ensure that the visitor completes the security access log for the area. Under no circumstances may anyone be within the confines of the OIT data center without either a valid ID badge or an entry to the security access log for the area.

Any L&I User granting access to the secured area is responsible for any violations of OIT's security protocols that may occur as a result of granting such access. Under no circumstances shall a visitor be without an escort displaying an ID badge while in OIT data centers.

Tours and other types of groups must be escorted through the restricted area, and such groups' access to the secured areas will be controlled by the L&I User who is escorting the group(s). Every visitor who is part of a tour or group is required to complete the security access log.

5. Responsibilities:

A. L&I User responsibilities:
- Display their ID badge at all times while in an OIT secured area;
- Ensure tailgating/piggybacking, does not occur;
- Be prepared to present their ID badge upon request;
- Not give or loan their ID badge to another individual;
- 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:
- Contact OIT Security for access removal when L&I Users who are under their supervision are departing;
- Ensure non-IT equipment is not stored in OIT secured spaces;
- 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 physical security.

6. References:

L&I Policy Definitions Document

L&I SEC-004 - Computer and Information Security

ITP SEC029 - Minimum Standards for Improving Physical Security Access

Management Directive 625.10 - Card Reader and Emergency Response Access to Certain Capitol Complex Buildings and Other State Office Buildings

7. Version Control:

Version	Date	Purpose
2.0	01/10	Updated
2.1	05/2016	Updated to new policy format
2.2	07/2017	Annual review & content update