pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-004

Name:	Computer and Information Security
Effective Date:	June 2017
Category:	Security
Version:	1.2

1. Purpose:

This policy establishes standards by which all Department of Labor & Industry (L&I) data, applications, and systems will operate in compliance with all applicable local, state, and federal laws and regulations. This policy defines the roles and responsibilities of users in relation to information and cyber security to raise awareness of potential risks associated with the use of information technology.

This policy provides direction and identifies guidelines regarding cybersecurity, as well as computer and information security; fulfills requirements of Internal Revenue Service (IRS) Publication 1075; and implements the safeguards and requirements defined by the Social Security Administration (SSA).

This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-20, CA-2, CA-3, SA-5, SA-8, and SC-28 Per SP 800-53 R4.

2. Background:

L&I information is a valuable asset and must be protected from unauthorized access, disclosure, modification, or destruction. L&I's Office of Information Technology (OIT) has implemented defense in depth security controls such as authentication and access controls that grant only the necessary access using the least privilege model, in order to minimize the costs of security breaches. Computer and Information security is an integral part of sound management and mission success for L&I. Adhering to this policy will reduce the risk of sensitive data being compromised and ensure that all agency systems are operating in the most secure state possible.

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:

OIT shall align security controls, policies, and practices with business requirements to support the missions of L&I.

OIT shall protect information used to conduct the business of L&I from unauthorized disclosure, use, modification, or destruction in accordance with industry best practices and in compliance with federal and state laws and regulations, including but not limited to IRS, SSA, and accepted security standards. OIT shall protect information at rest using encryption methods in compliance with ITP SEC020.

OIT shall establish and manage an overall information security program for the protection of L&I computers, networks, and information assets. OIT shall implement information security policies, standards, and best practices to ensure that the integrity, confidentiality, and availability of information used to conduct the business of L&I is not compromised.

OIT shall provide security requirements for the development of new application systems, and assure the consistent implementation of controls for information systems throughout the organization in accordance with the Governor's Office of Administration's (OA) standards and policies, as well as all state and federal laws.

OIT shall conduct regular security assessments including internal audits and external assessments of mission critical applications annually and non-mission critical applications every two years.

OIT shall conduct a review of application/system design per APP-000 and SEC-000, for changes that impact the security controls.

OIT management will review all purchases of IT equipment, software, and IT services to ensure that offerors are aware of and will comply with all security policies and standards per PLT-001.

The L&I Chief Information Security Officer (CISO) shall review policies and controls to address risks and specific compliance requirements for the agency. Easy to understand, effective, and enforceable policies shall be developed that balance protection with productivity in accordance with ADM-001. OIT management shall conduct annual reviews of written procedures to ensure continued compliance with security policies and standards.

The CISO, in conjunction with other OIT staff, shall be responsible for ensuring the implementation of an information security infrastructure that ensures the confidentiality, availability, and integrity of L&I's information assets. The CISO will serve as the primary point of contact to the agency Chief Information Officer/Deputy Chief Information Officer (CIO/DCIO) for all information technology security matters.

The CIO/DCIO, in conjunction with the CISO, shall periodically review operational information security breaches reported, identify possible new vulnerabilities, evaluate the effectiveness of related policies, standards, and practices, and propose updates.

The CIO/DCIO, CISO, and Office of Chief Counsel shall review data sharing agreements and trust relationships between L&I and any business partner or contracted resource owning, operating, or maintaining external information systems connected to L&I's systems. Data sharing agreements shall consist of documentation for each connection, including the data classification, interface characteristics, security requirements, data owner, and the nature of the information communicated.

5. Responsibilities:

A. L&I User responsibilities:

- Complete the mandatory security awareness training;
- Comply with all L&I policies, management directives, and laws; and
- Report any violations of policies promptly to the L&I Chief 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 computer and information security.

6. References:

L&I Policy Definitions Document

ADM-001 - OIT Policy and Procedure Development, Review, and Approval

ADM-002 - ITIL Compliance

APP-000 – System Development Life Cycle

PLT-001 - Purchase Deployment and Transportation of IT Equipment

SEC-000 - Security Planning Policy

SYM-001 - Contingency Planning & Training Policy

ITP SEC016 - Commonwealth of Pennsylvania - Information Security Officer Policy

ITP SEC020 - Encryption Standards for Data at Rest

NIST SP 800-53 R4 – NIST 800-53

7. Version Control:

Version	Date	Purpose
1.0	06/2007	Base Document
1.1	05/2016	Updated to new policy format
1.2	06/2017	Annual review & content revision