pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Plan

Name:	System Security Plan
Effective Date:	June 2017
Category:	Security
Version:	1.1

1. Scope:

This plan applies to all Department of Labor & Industry (L&I) system owners (SO), and Office of Information Technology (OIT) employees and business partners (hereinafter referred to collectively as "L&I Users").

2. System Security Plan:

The System Security Plan (SSP) must, at a minimum, include these items:

1. Information System Name/Title:

   Unique identifier and name given to the system.

2. Information System Categorization:

   Identify the appropriate FIPS 199 categorization and data owner

3. Information System Owner:

   Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official:

   Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts:

   List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility:

   Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status:

   Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

   (Operational | Under Development | Major Enhancement)

8. Information System Type:

   Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.

pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Plan

(Major Application | General Support System)

9. General System Description/Purpose

   Describe the function or purpose of the system and the information processes.

10. System Environment

    Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

11. System Interconnections/Information Sharing

    List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, CA2 status, and the name of the authorizing official.

    (System Name | Organization | Type | Agreement (ISA/MOU/MOA) | Date | FIPS 199 Category | CA2 Status | Auth. Official)

12. Related Laws/Regulations/Policies

    List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

13. Minimum Security Controls

    Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from NIST SP 800-53. Then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain:

    1) the security control title;

    2) how the security control is being implemented or planned to be implemented;

    3) any scoping guidance that has been applied and what type of consideration; and

    4) indicate if the security control is a common control and who is responsible for its implementation.

14. Expected user behavior

    Roles and access levels for the system

    Roles and access levels for the data

15. Information System Security Plan Completion Date: _____

16. Information System Security Plan Approval Date: _____

L&I, Office of Information Technology Plan

3. References:

L&I Policy Definitions Document

SEC-000 Security Planning Policy

4. Version Control:

Version	Date	Purpose
1.1	10/2016	Base Document