pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SYM-001

Name:	Contingency Planning & Training Policy
Effective Date:	December 2016
Category:	System Management
Version:	1.1

1. Purpose:

This policy defines the requirement for contingency planning to be developed and implemented by the Department of Labor & Industry (L&I). These contingency plans will describe the processes to recover Information Technology (IT) Systems, Applications and Data from any type of disruption or disaster. This policy also provides directions and identifies guidelines regarding Disaster Recovery(DR), fulfilling the requirements of the Internal Revenue Service (IRS) Publication 1075, and NIST CP-2-5 Per SP 800-53 R4 as well as safeguards and requirements defined by the Social Security Administration (SSA).

2. Background:

This policy is published under the general authority of the Governor's Office of Administration / Office of Information Technology (OA/OIT) in conjunction with IRS Publication 1075 in that it identifies key roles and responsibilities regarding contingency planning and training. IRS Publication 1075 provides direction regarding acceptable contingency planning and training standards to help ensure that the agency is prepared and equipped to handle future events or circumstances.

All Federal Tax Information (FTI) that is transmitted to L&I is backed up and protected within IRS facilities ensuring availability in the event of a disruption or disaster, including cyberattack. L&I's contingency planning controls for FTI will be focused on the confidentiality and integrity of FTI stored in backup media or used at alternative facilities. L&I will develop applicable contingencies for ensuring that FTI is available based upon L&I's risk-based approach. L&I will also develop contingencies for the restoration of other services as quickly as 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:

A. Contingency Plans

L&I Office of Information Technology (OIT) and L&I business area management will develop a Contingency Plan (CP) for each system.

L&I OIT will work with the business areas within L&I to rate each application according to a Business Impact Analysis (BIA) annually. The BIA will be conducted for each business area application to evaluate the business critical function, Maximum Tolerable Downtime (MTD), Return to Operation (RTO) timeline, Recovery Point Objective (RPO), capacity requirements, and current DR Plan. The BIA will determine systems and their order on the Mission Critical Applications (MCA) list.

L&I OIT will work with the Continuity of Operations Planning (COOP) Coordinator to develop communications plans for an MCA outage and cyberattack, and review these annually.

L&I OIT will develop an order of succession plan for each bureau, division and section in support of the MCAs, and will review these annually with the COOP Coordinator.

L&I OIT must work with the business areas within L&I to categorize data per OA ITP-SEC019

L&I OIT will develop internal DR procedures for the recovery of all MCAs based on agreed upon RTO and RPO standards. These DR procedures will be reviewed annually or when there is a significant change in the architecture or infrastructure supporting the MCA.

B. Contingency Training

All CP and DR plans must be tested annually to validate the plan and train staff.

Training exercises can consist of tabletop exercises, DR tests, up to partial or full transition of production services to the DR site. The business area and OIT will jointly determine the schedule and extent of the training exercise.

All contingency plans and DR training exercises will include an After Action Review (AAR), which will be recorded with the results of the training. Failures or unsuccessful tests must be documented and be part of the next successive CP or DR test.

Documentation of all tests including a synopsis of the exercise and AAR will be saved with each MCA contingency plan for review by the COOP Coordinator.

5. Responsibilities:

A. L&I User responsibilities:

- Comply with all established OIT policies.
- Adhere to all established CP policies and procedures.
- Participate in CP and DR testing and training exercises as required.

B. L&I management responsibilities:

- Ensure that users comply with all established OIT policies.
- Follow this policy and any procedures regarding contingency planning or training.
- Ensure L&I Users comply with all L&I policies.

6. References:

L&I Policy Definitions Document

OA ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data

Management Directive 205.41 Commonwealth of Pennsylvania Continuity of Operations (COOP) Program

Executive Order 2012-05 Commonwealth Continuity of Government

IRS Publication 1075

SP 800-53 R4 Security Controls and Assessment Procedures for Federal Information Systems and Organizations

7. Version Control:

Version	Date	Purpose
1.0	10/2016	Base Document
1.1	12/2016	Content additions and edits