pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Procedure

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

1. 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.

2. Procedure:

This procedure is implemented by various L&I Users from both the Office of Information Technology (OIT), Bureau of Human Resources (BHR) and the business units. This procedure will be initiated by the Chief Information Security Officer (CISO) and Enterprise Security and Compliance Section (ESC) at the direction of the Chief Information Officer (CIO) and Deputy CIO (DCIO). Steps will additionally be completed by the Business Relationship Management (BRM) division, and Enterprise Architecture and Standards section (EAS).

A. Contingency Planning
Conducted when required by information system changes and no less than annually.

Step	**Responsibility**	**Action**
1.	CISO/ ESC / BRM / EAS	Update Mission Critical Applications (MCA) list
2.	CISO/ ESC / BRM / EAS	Coordinate Business Impact Analysis (BIA) to determine: • Maximum Tolerable Downtime (MTD) • Return to Operation (RTO) timeline • Recovery Point Objective (RPO) • Capacity requirements
3.	ESC / BRM/ EAS/ COOP	Coordinate review and update of Contingency Plan (CP) with business area
4.	CISO/ ESC / BRM / EAS	Coordinate review and update of Disaster Recovery (DR) plan with business area
5.	CISO/ ESC	Coordinate review of communications plans for MCA outage and cyberattack with Continuity of Operations Planning (COOP) Coordinator in BHR
6.	CIO/DCIO	Coordinate review and update of OIT bureau succession plans

7.	BRM/ COOP	Coordinate review and update of business area succession plans

B. Contingency Training
Conducted when required by information system changes and no less than annually.

Step	Responsibility	Action
1.	CISO/ ESC / BRM	Coordinate CP testing
2.	BRM	Conduct After Action Review (AAR) following CP testing
3.	BRM	Store CP documentation, test results and CP test AAR with CP and share with COOP coordinator
4.	CISO/ ESC / BRM	Coordinate DR Plan testing
5.	BRM	Conduct After Action Review (AAR) following DR testing
6.	BRM	Store DR documentation, test results and DR test AAR with DR plan and share with COOP coordinator

3. References:

SYM-001 Contingency Planning & Training Policy

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

4. Version Control:

Version	Date	Purpose
1.0	06/2016	Base Document
1.1	12/2016	Content additions and edits