pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SYM-005

Name:	Backup Policy
Effective Date:	April 2017
Category:	System Management
Version:	1.1

1. Purpose:

This policy identifies guidelines for backup, storage, retention, security, confidentiality availability, integrity, and restoration of data processed or stored by the Department of Labor & Industry (L&I). This policy provides direction for data and system owners regarding the parameters of and controls applied to data backup and restoration. This policy establishes guidelines for the identification, collection, and search of electronically stored information (ESI) for purposes of electronic discovery (e-discovery) in litigation matters. This accountability will help protect information, including Federal Tax Information (FTI), from unauthorized access and improper disclosure in compliance with safeguards and requirements defined by the Internal Revenue Service (IRS) and the Social Security Administration (SSA). This policy also identifies guidelines regarding Information System Backup, fulfilling the requirements of the IRS Publication 1075, and NIST critical controls: CP-4, CP-6, and CP-9 Per SP 800-53 R4

2. Background:

This policy is published under the general authority of the Office of Information Technology (OA/OIT).

L&I OIT has measured significant cost and waste in the current backup model, and is updating the standards for backup to dramatically reduce the costs of backups and improve the supporting service of backups.

All 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 also develop contingencies for the restoration of other services as quickly as possible.

As a business function and best practice, L&I will conduct, store, and secure backups of data for Mission Critical Applications (MCA) as well as other services and systems in order to meet legal, business, and operational requirements as well as reduce down time and achieve recovery objectives.

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").

L&I, Office of Information Technology Policy SYM-005

4. Policy:

L&I system owners (SO) shall define all environments and the backup requirements for each environment with OIT.
L&I SO shall define the classification of the data to be backed up for each system.
L&I OIT shall align backup strategy with business needs and compliance requirements.
L&I OIT shall treat all data and records about L&I data as an asset of the agency.
L&I OIT shall conduct backups and maintain the integrity of user-level, application-level, and system-level information and security-related data.
L&I OIT shall document the standard backup retention period and frequency intervals for each environment: (Development (DEV), Component Integration Testing (CIT), User Acceptance Testing (UAT), and Production (PROD)).
L&I OIT shall document and maintain procedures on the backup and recovery of information systems data.
L&I OIT shall provide role based access controls for access to and the restoration of backup data.
L&I OIT shall ensure the proper logical security controls are in place to protect the confidentiality, integrity, and availability of backup information at storage locations.
L&I OIT shall employ physical controls to protect system backups from tampering or exploitation, including encrypted backup files, secured transport, offsite storage, and tape recovery.
All backups for systems shall be encrypted to comply with NIST standards, and OA ITP-SEC020 Encryption Standards for Data at Rest.
L&I OIT shall provide secured storage of backups in transit to offsite locations per OA ITP-SEC031 Encryption Standards for Data in Transit.
L&I OIT shall document frequency standards, retention period, backup procedures, and recovery procedures for Disaster Recovery (DR) and Continuity of Operations (COOP) per L&I OIT SYM-001. Secured backups shall be provided as part of the program area DR and COOP plans.
L&I Office of Chief Council (OCC) shall notify the agency Chief Information Security Officer (CISO) as early as possible, data that must be identified, collected, searched, preserved, or analyzed as ESI.
L&I OIT shall take direction from the OCC and the agency CISO to allow or deny access to non-commonwealth entities involved in the identification, collection, and analyzation of ESI.
L&I OIT shall coordinate with OCC for all ESI and e-discovery related to litigation holds or Records Legal Hold.
L&I OIT shall not dispose of any record that are subject to a records legal hold or that are reasonably likely to be involved in litigation without the approval from the L&I OCC.

5. Responsibilities:

A. L&I User responsibilities:

- Notify OIT operations staff for variances to backup strategy as required;

- Adhere to all established backup policies and procedures;
- Preserve all ESI identified as part of an e-discovery for litigation hold; and
- Comply with all established OIT policies.

B. L&I management responsibilities:

- Follow this policy and any procedures regarding the backup of L&I data; and
- Ensure that users comply with all established OIT policies.

6. References:

L&I Policy Definitions Document

SYM-001 Contingency Planning & Training Policy

OA ITP-INF000 Enterprise Data and Information Management Policy

OA ITP-INF009 e-Discovery Technology Standard

OA ITP-SEC020 Encryption Standards for Data at Rest

OA ITP-SEC031 Encryption Standards for Data in Transit

MD 210.5 - The Commonwealth of Pennsylvania State Records Management Program

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	02/2009	Base Document
1.1	04/2017	Format and Content Revision