pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

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

Name:	System Maintenance Policy
Effective Date:	May 2017
Category:	System Management
Version:	1.2

1. Purpose:

This policy provides direction and identifies guidelines regarding system maintenance policies; fulfills the requirements of Internal Revenue Service (IRS) Publication 1075; and implements the safeguards and requirements defined by the Social Security Administration (SSA).

2. Background:

This policy is published under the general authority of the Office of Administration / Office of Information Technology (OA/OIT) in conjunction with IRS Publication 1075 in that it identifies key roles and responsibilities regarding system maintenance. IRS Publication 1075 provides direction regarding acceptable system maintenance standards for local and non-local systems, as well as the maintenance personnel performing system maintenance. The Department of Labor & Industry (L&I) Office of Information Technology (OIT) monitors the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and United States Computer Emergency Readiness Team (US-CERT) for new vulnerabilities and patches to mitigate them. 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. This policy will document the implementation of the National Institute of Standards and Technology NIST Security Controls: MA-1, 2, 3, 4, 5, & 6 per SP 800-53 R4.

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").

4. Policy:

A. System Maintenance:

L&I OIT shall develop, document, and disseminate controls over system maintenance.
L&I OIT shall review and update the controls over system maintenance annually.
L&I OIT shall implement automation to deploy and monitor patch management on all servers, workstations, and mobile devices. All servers, workstations, and mobile devices shall be maintained using these automation tools and controls.
L&I OIT shall establish scheduled scans of application inventories in compliance with PLT-004 Inventory of Authorized & Unauthorized Hardware & Software. Deviations from this schedule must be documented with a waiver following the L&I Change Management process.

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

L&I OIT shall take actions in response to weekly reports from OA/IT anti-virus support to mitigate systems that have neither connected to the network or received an update.
L&I OIT shall conduct monthly scans for missing updates within one (1) business day following the scheduled server patch cycle.
L&I Users shall connect their workstation to the L&I network every two weeks or 10 working days for no less than two hours for system updates and patching.
L&I OIT shall comply with the timelines documented in ITP-SYM006.

B. Security Maintenance:

L&I OIT shall document procedures for the deployment of security patches outside of normal change windows.
L&I OIT shall monitor for new vulnerabilities that have been recorded by the NIST NVD and US-Cert.
L&I OIT shall report all applicable "Critical/High" NVD and US-Cert vulnerabilities to IT Equipment administrators and system owners.
All IT equipment administrators and system owners shall report to the L&I CISO within one (1) business day of receiving a report of an applicable "Critical/High" NVD or US-Cert vulnerability, the mitigation of the vulnerability, scheduled date for mitigation, or anticipated delivery of security vulnerability patches.

C. Non-Local System Maintenance:

L&I OIT shall establish authorized maintenance and diagnostic tool sets for IT Equipment and systems consistent with SEC-010 Access Control for Non-Commonwealth Users Policy, SEC-011 Remote Access to the Commonwealth Network Policy, and PLT-004 Inventory of Authorized & Unauthorized Hardware & Software Policy.
L&I OIT shall employ multi-factor authentication in the establishment of non-local maintenance and diagnostic sessions.
L&I OIT shall document all non-local maintenance activities following the L&I Change Management Process.
L&I OIT shall monitor and log all non-local maintenance and diagnostic activities.
L&I OIT shall retain all logs and records for non-local maintenance and diagnostic activities as an auditable record per SEC-012 Audit and Accountability Policy.
L&I OIT shall establish controls to terminate sessions and network connections when non-local maintenance is completed.

D. Maintenance Personnel:

L&I OIT shall establish a process for authorizing L&I Users to perform local and non-local maintenance. No L&I User shall be granted elevated privileges without following the L&I Change Management process.

L&I OIT shall maintain records of L&I Users with elevated privileges on IT Equipment and systems. All changes to privileges of an L&I User must follow the L&I Change Management process.
L&I OIT shall not grant access to L&I Users without required authorizations. All local maintenance L&I users who have not been vetted shall be escorted per SEC-006 OIT Secured Area Access and Physical Security Policy.
L&I OIT shall designate personnel with required access authorizations and technical competence to supervise the maintenance activities of L&I Users who do not possess the required access authorizations.

5. Responsibilities:

A. L&I User responsibilities:

- Connect their workstation to the L&I network at least every two weeks or 10 working days for no less than two hours for system updates and patching;
- Comply with all L&I policies, management directives, and laws; and
- Report any violations of policies promptly to 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 configuration management.

6. References:

L&I Policy Definitions Document

Out of Band Patching Procedure v1.2

Standard System Patching

PLT-004 Inventory of Authorized & Unauthorized Hardware & Software

SEC-006 OIT Secured Area Access and Physical Security

SEC-010 Access Control for Non-Commonwealth Users Policy

SEC-011 Remote Access to the Commonwealth Network

SEC-012 Audit and Accountability Policy

OA ITP-SEC035 Mobile Device Security Policy

OA ITP-SYM006 Commonwealth IT Resources Patching Policy

United States Computer Emergency Readiness Team (US-CERT)

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base Document
1.1	04/2017	Format and Content Revision
1.2	05/2017	Updates based on policy changes