pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

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

Name:	Mobile Device Usage
Effective Date:	July 2017
Category:	Network
Version:	1.2

1. Purpose:

This policy defines acceptable use of mobile devices issued to employees by the PA Department of Labor & Industry (L&I). This policy mitigates the risks of improper use and handling of mobile devices that can result in the loss or compromise of Commonwealth information or subject Commonwealth information systems to malicious software, programs, or code.

This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-19, SC-18 Per SP 800-53 R4

2. Background:

This policy is published under the general authority of the ITPs published by the Governor's Office of Administration/Office of Information Technology (OA/OIT), in that it identifies key roles and responsibilities in support of ITPs.

Inappropriate use of mobiles devices can result in a data breach or loss of sensitive information to untrustworthy sources. Such breach or loss could result in loss of service, loss of state or federal funding, or place L&I at risk of legal and financial repercussions. The L&I Office of Information Technology (OIT) is responsible for the protection of all devices that store and communicate Commonwealth or L&I data, including mobile devices.

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:

OIT is responsible for the management of mobile devices issued by L&I.

L&I Users shall only use mobile devices issued by L&I for Commonwealth business purposes.

L&I Users may not use a mobile device issued by L&I in any way which is inconsistent with Commonwealth or L&I policy, including policies regarding availability, capability, or inappropriate content of communications.

OIT will install a Mobile Device Management (MDM) software on all devices in accordance with ITP-SEC035, before deployment to L&I Users. The MDM solution monitors all mobile devices and reports on apps that have not been approved for use.

L&I users may not remove the MDM app from their mobile device. L&I users may not change the AppleID, the AppleID password or any other information assigned to the mobile device. L&I Users may not log into the device using any AppleID other than the one assigned by OIT.

Only applications (apps) that have been approved by the L&I Software Review Committee (SRC) may be installed by L&I Users. Authorized apps can be downloaded through the L&I "App Catalog" on the device.

OIT shall notify users with unauthorized apps to uninstall the app.

L&I Users shall have two business days to remove the app. If the app is not removed, OIT will send a notification to the user's manager/supervisor.

L&I Users shall submit requests for new apps, not available in the app catalog, to the OIT Software Review Committee (SRC). Requests for apps not currently available through the L&I app catalog must be submitted via service catalog request, approved by the requestor's management, and submitted to and approved by the SRC.

L&I Users may not install any app that is considered inappropriate for work, such as one containing explicit sexual material.

OIT will immediately remove all apps that are categorized as malicious, inappropriate, or potentially harmful to the device, the user, or to Commonwealth data stored on the device.

L&I Users may not store Commonwealth or L&I data on non-Commonwealth/L&I mobile devices without authorization by the agency chief information officer and the deputy secretary with operational responsibility.

The connection of a non-Commonwealth/L&I issued device to the Commonwealth network must be authorized by the deputy secretary with operational responsibility and secretary of L&I in accordance with Management Directive MD 240.11. Approved Non-Commonwealth/L&I issued mobile devices connected to Commonwealth/L&I IT resources are subject to compliance with the Right to Know Law.

All L&I Users who are issued a mobile device shall read, agree to, and sign the OIT-5 Computer Resources User Agreement - Commonwealth Employees or the OIT-6 Computer Resources User Agreement - Non-Commonwealth Employees prior to being issued a mobile device and annually thereafter. OIT shall notify the Bureau of Human Resources/Employee Relations (BHR/ER) upon any violation of this policy.

OIT will work closely with (BHR/ER) to communicate appropriate behavior for mobile device usage.

5. Responsibilities:

A. L&I User responsibilities:

- Comply with all L&I policies, management directives, and laws; and

- Report any violations of policies promptly to the L&I Chief Information Security Officer at 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 mobile devices.

6. References:

ITP-SEC024 IT Security Incident Reporting Policy

ITP-SEC035 Mobile Device Security Policy

MD 240.11 Commonwealth Wireless Communication Policy

MD 240.12 Commonwealth of Pennsylvania Mobile Device Security Policy

MD 205.34 Information Technology Acceptable Use Policy

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base Document
1.1	08/2016	Format and Content Revision
1.2	06/2017	Format and content revision for NIST compliance