L&I, Office of Information Technology Policy SEC-010

<table>
<thead>
<tr>
<th>Name:</th>
<th>Access Control for Non-Commonwealth Users Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>November 2016</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Version:</td>
<td>2.1</td>
</tr>
</tbody>
</table>

1. **Purpose:**

To specify the access controls and expected behavior regarding non-commonwealth users (hereinafter “contractors”) and their access to Department of Labor & Industry (L&I) Information Technology systems and data. This includes contractors working directly with L&I’s Office of Information Technology (OIT) staff, as well as external support entities.

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 Section 9.3 Access Control](https://www.irs.gov/publications/p1075). L&I systems are protected by robust security measures in order to protect L&I’s applications and information. Granting contractors elevated privileges to L&I production (PROD) systems could potentially compromise them. Without the proper safeguards and controls in place, L&I OIT staff may not be able to replicate, correct, or explain the matter. L&I PROD applications are valuable, sometimes mission critical, assets. Therefore, every possible measure must be taken in order to ensure their protection and maintenance.

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 “Users”).

4. **Policy:**

L&I OIT staff will ensure only the necessary level of access is requested for contractors.

Contractors at L&I will not be given elevated or privileged account access to any L&I Production (PROD) environment without approvals following the procedures described in Access Control for Non-Commonwealth Users Procedures.

Contractors must access all L&I systems using their unique domain logon credentials. The use of anonymous, guest, or service accounts by contractors is forbidden and will be considered a security breach, without an exception following the Access Control for Non-Commonwealth Users Procedure.

Contractors must document all actions and activates on PROD systems.

Contractors must provide knowledge transfer to L&I Users to ensure familiarity with all systems, processes and activities so they may troubleshoot any issues that may arise.
L&I, Office of Information Technology Policy SEC-010

Contractors must supply all supporting documentation in accordance with Access Control for Non-Commonwealth Users Procedures.

Contractor accounts with elevated privileges will be reviewed annually.

5. Responsibilities:

A. L&I User responsibilities:
   - Comply with all security policies, management directives and laws.
   - Report any violations of policies promptly to LI, OIT-DLICISO.

B. L&I management responsibilities:
   - Comply with all L&I policies and ensure employees comply with the policies.
   - Adhere to Access Control for Non-Commonwealth User Procedures.

6. References:

   L&I Policy Definitions Document
   SEC-007 - Contractor Account Administration
   SEC-011 - Remote Access to the Commonwealth Network
   MD205.34 - Commonwealth of Pennsylvania IT Acceptable Use Policy
   ITP_SEC009 - Minimum Contractor Background Checks Policy
   ITP_SEC010 – Virtual Private Network Standards

7. Version Control:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>02/2012</td>
<td>Base Document</td>
</tr>
<tr>
<td>2.0</td>
<td>10/2015</td>
<td>Combined 340 with 340.1 and added content</td>
</tr>
<tr>
<td>2.1</td>
<td>11/2016</td>
<td>Format and content revision</td>
</tr>
</tbody>
</table>