

L&I, Office of Information Technology Policy SEC-011

Name:	Remote Access to the Commonwealth Network
Effective Date:	June 2017
Category:	Security
Version:	1.2

1. Purpose:

This policy establishes standards by which all Department of Labor & Industry (L&I) users will request remote access to the commonwealth network, provides management direction regarding remote access requests, and protects the confidentiality and integrity of commonwealth data and infrastructure. Remote access is provided by the Governor’s Office of Administration (OA) and supported by L&I’s Office of Information Technology (OIT). This policy is meant to promote improved operational efficiency, increased productivity, reduced security risks, consistent technical support, and availability of services. This policy documents the implementation of the National Institute of Standards and Technology ([NIST Security Controls](#): AC-1, 3, 4, 17, 18, 19, 20, IA-2, IA-3, 5, & 8 Per [SP 800-53 R4](#)).

2. Background:

This policy is published under the general authority of the ITPs published by OA/OIT, in that it identifies key roles and responsibilities in support of ITPs. This policy is in addition to the OA policy [ITP-SEC010](#).

L&I OIT provides remote connectivity to the L&I network for users who routinely work from home. Remote connectivity may also be provided for extenuating circumstances such as:

- Pandemic preparedness and emergency/disaster scenarios.
- Critical systems support during off hours.
- Employees with immediate, pressing deliverables that need to be completed, but who are unable to make it to the work location.
- Agency testing and piloting of mobile workforce initiatives.

3. Scope:

This policy applies to all L&I employees, business partners, contractors, temporary personnel, agents, and vendors who have been provided an L&I asset, access to connect, or are already connected remotely to the L&I network (hereafter referred to collective as “L&I Users”).

4. Policy:

A. Authorization:

L&I Users desiring remote access privileges via Virtual Private Network (VPN) are required to submit a Change Request (CR), through their ServiceNow submitter for approval by their direct supervisor and bureau director.

L&I, Office of Information Technology Policy SEC-011

L&I Users shall submit the CRs two (2) weeks in advance of the requested implementation date. However, if a program area submits a "Critical" priority CR, OIT will expedite the processing of the CR with OA.

OIT shall not provide access privileges without an approved CR.

B. Eligibility:

L&I Users shall only be granted remote access to the commonwealth's network if the following conditions have been met:

- i. The remote access is being provided for an L&I User who needs to work from home or work without a stationary place of business; and
- ii. The remote access being provided is on IT Equipment with the necessary technology and security controls in place.

C. Access Controls and Security Measures:

- i. OIT staff shall be responsible for adding, changing, and deleting remote access for L&I Users.
- ii. Remote access is based on User ID, password, and secure ID authentication. A 'digital certificate' will need to be obtained from OA to secure ID authentication.
- iii. OA/OIT has implemented a client-side agent that performs device compliance checks, such as anti-virus validation, to mitigate security risks before users are authenticated and granted remote access. Access shall not be obtained without passing this step.
- iv. OIT shall be responsible for ensuring that commonwealth workstations have disk encryption installed and enabled before the installation of the VPN software.
- v. OA/OIT shall restrict access to network resources and data on the commonwealth network with VPN 'user groups'. All access provided is through the firewalls of the commonwealth and L&I.
- vi. L&I program areas authorize access to their own applications.
- vii. OIT shall monitor remote access for unauthorized access attempts or activity.

D. Internet Access:

The L&I User or L&I may provide Internet access. If L&I provides Internet access, the selection of and contracting with an Internet Service Provider (ISP) are the responsibility of OIT. If the L&I User provides Internet access, the L&I User is solely responsible for the selection of an ISP and any associated expenses.

E. Termination of Remote Access Privileges:

- i. The commonwealth may choose to terminate remote access privileges at any time.

L&I, Office of Information Technology Policy SEC-011

- ii. These privileges shall automatically end when L&I User accounts are locked at the end of their services for L&I.
- iii. Remote user access privileges may be disabled or deleted from the system after extended periods without use.
- iv. L&I User access privileges shall be re-evaluated whenever there is a change in job responsibilities.
- v. OIT shall remove workstations from domain membership that have not connected to the domain in 60 days

5. Responsibilities:

A. L&I User responsibilities:

- Maintain endpoint checks and prerequisites per [ITP_SEC010](#); and
- 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; and
- Adhere to the same commonwealth business-use rules that apply to a direct network connection when using a remote connection; and
- Ensure proper security measures are taken to prevent unauthorized access to the commonwealth's network and data; and
- Follow all instructions from OIT.

B. L&I management responsibilities:

- Review requests for remote network access and authorize where appropriate;
- Ensure funding for the VPN service is available; and
- Provide funding for commonwealth-provided Internet access where it has been approved.

6. References:

[L&I Policy Definitions Document](#)

[SEC-007](#) - Contractor Account Administration

[SEC-010](#) - Access Control for Non-Commonwealth Employees Policy

[SYM-004](#) - System Maintenance Policy

[ITP_SEC010](#) - Virtual Private Network Standards

7. Version Control:

<u>Version</u>	<u>Date</u>	<u>Purpose</u>
1.0	03/2009	Base Document
1.1	10/2016	Format and Content Revision

L&I, Office of Information Technology Policy SEC-011

1.2	06/2017	Updates based on policy changes
-----	---------	---------------------------------