Office of Information Technology Policy

ISSUE DATE: July 10, 2007	PAGE 1 OF 2	POLICY NO: C-306

SUBJECT: Application Access Control

APPROVAL AUTHORITY: Chief Information Officer

Authorization:

This policy is published under the general authority of the Security Domain Information Technology Bulletins published by the Office of Administration, Office of Information Technology (OA/OIT), in that it identifies key roles and responsibilities in support of Information Technology Bulletins (ITBs) relating to information security.

Purpose:

The purpose of this policy is to prevent unauthorized access to information held in Department of Labor & Industry (L&I) computing resources.

Scope:

This policy applies to all L&I employees, business partners, contractors, temporary personnel, agents, and vendors with access to information that is owned or controlled by L&I.

Any information held in an L&I computing resource should be protected from unauthorized access unless specifically designated for public dissemination. Unless specifically designated as a public access resource, all applications must have access controls in place that will protect information from unauthorized access.

User Access:

L&I computing resources that provide applications to users should have controls in place that limit application access to only those individuals who are properly designated. L&I Office of Information Technology (OIT) security management, in conjunction with impacted business areas, should base the designations of which users have access to specific applications on their business access control policies. In general, the day-to-day security administration of internal users (e.g., L&I employees) is handled by OIT security administrators. The day-to-day security administration of L&I business partners, or other third parties, is handled primarily by the impacted L&I business area in conjunction, as needed, with OIT security administrators.

Access to any application should be denied by default unless a need for access can be demonstrated. Individual users should be subject to specific controls, based on ownership of the information contained in or used by the application, that limit the user's rights to read, write, execute, and delete. Where resource ownership is shared, the rights to modify the data should be based on a business decision of L&I management.

System Configuration:

All L&I computing resources should protect against applications and utilities that have the ability to override application or system access controls. In addition, any system should be configured as follows:

1. To prevent compromising the applications or data of other systems it shares resources with;

2. To be able to limit access to information to only the owner of the information or other properly designated users and/or defined groups of users;
3. To provide a secured access to "system help" that provides information on how to override existing security measures; and
4. To provide controls that will limit the ability of the user to display, transmit, or use the output of any application only in ways approved by L&I management.

Public Access:

Where systems are providing access to L&I resources for the general public, the information designated as public should be segregated from all non-public resources in specially designated public domain resource configurations.

Policy Violations:

Violations of L&I's policies may result in disciplinary action up to and including termination of employment or contractor sanctions (including loss of e-mail, Internet, or computer access privileges).

Policy Interpretation:

This policy is issued in light of other guidance issued by OA/OIT, as well as existing laws, policies, and agreements of the Commonwealth of Pennsylvania. Where possible, this policy should be construed in a manner consistent with such other guidance, laws, policies, and agreements.

Questions concerning the interpretation of this policy, or any other OIT Policy, may be directed to ra-li-oit-policy@state.pa.us (LI, OIT-Policy).

References:

L&I/OIT Policies: C-305 - Information Access Control

OA/OIT ITB SEC013 - Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services