Office of Information Technology Policy C-340 REV

Subject: IT System Administration Guidelines for Non-Commonwealth Employees/Consultants

Approval Authority: OIT - Bureau of Enterprise Services, Security Division

Issue Date: 02/16/2012

Authorization

This policy is published under the general authority of the Information Technology Bulletins published by the Office of Administration / Office of Information Technology (OA/OIT), and incorporates the direction of those Information Technology Bulletins (ITBs) in relation to the availability of Labor & Industry (L&I) systems to Commonwealth-contracted personnel. As well, it incorporates the guidelines set forth by Management Directive 205.34 Commonwealth of Pennsylvania Information Technology Acceptable Use Policy.

Purpose

To specify the guidelines governing, and expected behavior regarding, access to Labor & Industry IT environments and information for non-Commonwealth Employees. This will be inclusive of contractors working directly with OIT staff, on vendor driven projects and external support vendors as it pertains to production system access.

Background

L&I environments and servers are consistently maintained with security protections to ensure the highest security posture available to protect the applications and information the Department handles on a daily basis. Granting administrative access to L&I production systems to contracted personnel provides the potential for those systems to be compromised by actions that Commonwealth staff may be unable to correct, replicate or properly explain on demand. Since L&I production applications, especially those which pertain to the citizens and the business entities of the Commonwealth of Pennsylvania, are valuable assets, we are required to take every possible measure to ensure their protection and proper maintenance.

Scope

This policy applies to all L&I employees, business partners, contractors, temporary personnel, agents, and vendors who have been provided with access to L&I's production systems.

Definitions

Environment – includes servers, networks, databases and applications that comprise a complete IT system.

Policy

Non-Commonwealth employees/consultants, such as staff augmentation contractors, project vendors and support vendor personnel at L&I will not be given administrative access to any L&I production environment without prior approvals from the Division Chief(s) over the affected environment or their designee and at least one member of the OIT Enterprise Change Control Board. For any personnel who are granted administrative access to these environments, access is to only occur through the individuals' unique logon IDs for direct system access. Use of anonymous, guest or service accounts is strictly forbidden and will be considered a security breach.

Elements that would be affected by this restriction include, but are not limited to:

- □ Servers
- □ Databases
- □ Applications
- □ Network components

In the event that administrative access to a production IT system has been approved for Non-Commonwealth or vendor support employees, proper measures must be taken to ensure the security and proper functioning of that environment and all of its components.

Additionally, unless a waiver is granted by the Enterprise Change Control Board, proper knowledge transfer to Commonwealth personnel must occur. This ensures that Commonwealth personnel are familiar enough with all engaged processes and activities to troubleshoot any issues that may arise as a result of the Non-Commonwealth personnel's actions. All changes to the environment by Non-Commonwealth personnel must strictly adhere to all OIT change management processes.

Responsibilities

- □ Agency Employees/Contractors: To abide by the restrictions outlined in this policy and report any violations of it promptly to ra-li-oit-dliciso@pa.gov (LI, OIT-Policy).

- □ Agency Management: To ensure that all staff understand the security policy as it is outlined and to assist in the enforcement of all L&I policies.

Policy Enforcement

Per Management Directive 205.34 (Commonwealth of Pennsylvania Information Technology Acceptable Use Policy):

> *Misuse of Commonwealth IT resources by employees or volunteers may result in disciplinary action, up to and including termination, depending on the circumstances of the incident. The improper use of Commonwealth IT resources by contractors or consultants may result in disciplinary action that may include formal action under the terms of the applicable contract or debarment under the Contractor*

> *Responsibility program. When warranted, the Commonwealth or its agencies may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws through the use of Commonwealth IT resources*.

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 may be referred to the DLI CISO and designees. These questions concerning the interpretation of this policy may be directed to ra-li-oit-dliciso@pa.gov (LI, OIT-Policy).

References

OA Management Directives:	MD205.34 - Commonwealth of Pennsylvania Information Technology Acceptable Use Policy