Information Technology Policy
Commonwealth of Pennsylvania
Governor's Office of Administration/Office for Information Technology

ITP Number:	**ITP-PLT012**	
ITP Title:	**Use of Privately Owned PCs to Access CoPA Resources**	
Issued by:	**Deputy Secretary for Information Technology**	
Date Issued: October 20, 2006		**Date Revised: December 20, 2010**
Domain:	**Platform**	
Discipline:	**Desktop/Laptop**	
Technology Area:	**Remote Access**	
Revision History Date:	**Description:**	
12/20/2010	**ITP Refresh**	

Abstract:
The policy contained in this Information Technology Policy (ITP) addresses the acceptable safeguards for use of privately owned computers to access the Commonwealth of PA (CoPA) network. Although it is not customary for users to access the CoPA network with a home-based personal computer (PC), allowances are to be made for extenuating circumstances such as:

- Pandemic preparedness and emergency/disaster scenarios.
- Agency testing and piloting of mobile workforce initiatives.
- 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.

General:
This ITP applies to all agencies, boards, commissions and councils under the governor's jurisdiction. Agencies not under the governor's jurisdiction are encouraged to follow this policy to ensure they develop and implement applications that facilitate enterprise-wide interoperability and standardization.

Policy:
This policy applies to employees or contractors who use a privately owned system, such as a home PC, to remotely access the CoPA network. This covers all forms of remote access including but not limited to: Outlook Web Access, access via Terminal Services (e.g., Citrix, Remote Desktop Protocol, and Virtual Private Network).

Please note that, although employees may use a home PC to remotely connect to the CoPA network, this in no way implies that the privately owned system will be supported by the Commonwealth. In addition, connecting privately owned
computers or computing devices directly to the CoPA network, including agency networks, is strictly prohibited.

For instances when an employee uses a privately owned computer to gain remote access to the CoPA network or CoPA applications, the following policy statements apply:

- Anti-Virus (AV) software is to be installed and kept current. If AV software is not already installed, it is recommended that employees utilize the McAfee AV software which is made freely available to all Commonwealth employees. AV software can be downloaded and installed by following the following directions found on the Cyber Security Portal. On the left toolbar select Log In, then select Commonwealth Employees and Employee Cyber Benefits . Follow the instructions provided. For additional information, please refer to ITP-SEC001 *Enterprise Host Security Suite Software Standards* for policy regarding McAfee AV.

- Patches and security updates are to be kept current in accordance with ITP-SYM006, *Desktop and Server Patching Policy.* For computers with a Microsoft operating system, it is recommended that the Microsoft Windows Update feature be configured to automatically receive and install updates.

- Employees who are working from home are to store and maintain all business-related data on the CoPA network. Commonwealth data is never to be saved locally to a home PC.

- "Public" computers (e.g., computers provided by libraries, universities, coffee shops, hotel business centers, etc. for general public use) are not be used to access the CoPA network. Using a public computer to connect to a Commonwealth owned network poses a significant security risk in that a third party may easily capture a user's logon credentials.

- If the personal computer used to remotely access CoPA is located on a home wireless network, then the wireless network is to be secured based on industry best practices (renaming the default SSID and utilizing WEP/WPA encryption, etc.). For more information regarding wireless network security, please refer to *Securing Wireless Networks*, provided by the United States Computer Emergency Readiness Team (US-CERT), at the following location: http://www.us-cert.gov/cas/tips/ST05-003.html.

- Home computers used to access the CoPA network are to adhere to the same minimum password requirements set forth by ITP-SEC007, *Minimum Standards for User IDs and Passwords*.

- Home users with a broadband connection are strongly encouraged to utilize a router, rather than connecting the computer directly to the Internet. Even low-end routers, which are often provided by many broadband ISPs, add Network Address Translation and firewall capabilities that provide a considerable amount of additional protection.

Refresh Schedule:

All standards identified in this ITP are subject to periodic review and possible revision, or upon request by the Enterprise Architecture Standards Committee (EASC).

Exemption from This Policy:

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be

entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required. Contact your agency CoP Planner for further details or assistance.

Questions:

Questions regarding this policy are to be directed to ra-itcentral@pa.gov.

References:

ITP-SYM006: Desktop and Server Patching Policy
ITP-SEC001: Enterprise Host Security Suite Software Standards ITP-SEC007: Minimum Standards for User IDs and Passwords Cyber Security Portal