pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Use of Privately Owned PCs to Access CoPA Resources

ITP Number	**Effective Date**
ITP-PLT012	October 20, 2006
Category	**Supersedes**
Platform	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	June 2017

1. Purpose

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.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Background

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.

4. 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 IT Central – Security/Anti-Virus (COPA ID access only). For additional information, please refer to ITP-SEC001 *Enterprise Host Security Suite Software Standards and Policy* for policy regarding anti-virus software.

- 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: https://www.us-cert.gov/security-publications/using-wireless-technology-securely

- 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, Passwords, and Multi-Factor Authentication.*

- 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.

NOTE: With Windows 10 Operating System, Microsoft has enhanced its feedback and diagnostic capabilities to include the automatic collection of information about a user's PC and the applications the user uses and the transmission of this information back to Microsoft. It is possible that this information could contain documents or other application data that the user was working on at the time a problem occurred. This could have the potential for a breach of the user's or the commonwealth's data, though Microsoft assures that this data will be used only for troubleshooting purposes by itself and its affiliates.

It is not possible to totally opt out of this functionality. However, through the **Diagnostic and usage data** settings (accessible through the Windows Control Panel), the user can minimize the data collected and sent off to Microsoft. We recommend the user familiarize with this Microsoft program and its options for participation in it. Microsoft has published a FAQ on this that is available at Windows 10 feedback, diagnostics, and privacy: FAQ.

5. Related ITPs/Other References

- ITP-SEC001 *Enterprise Host Security Suite Software Standards and Policy*
- ITP-SEC007 *Minimum Standards for User IDs, Passwords, and Multi-Factor Authentication*
- ITP-SYM006 *Desktop and Server Patching Policy*
- US-CERT Wireless Security - https://www.us-cert.gov/security-publications/using-wireless-technology-securely

6. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

7. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

8. 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.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	10/20/2006	Base Document
Revision	12/20/2010	ITP Refresh
Revision	06/06/2016	ITP re-format Updated URLs Updated References Added Note regarding Windows 10