pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Use of Privately Owned Devices to Access IT Resources

ITP Number ITP-PLT012	**Effective Date** October 20, 2006
Category Platform	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** October 2022

1. Purpose

This Information Technology Policy (ITP) addresses the acceptable safeguards for use of Privately Owned Devices to access Commonwealth of Pennsylvania (CoPA) IT Resources.

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

This policy applies to Authorized Users who use a Privately Owned Device, such as a home PC, to remotely access CoPA IT Resources.

3. Background

Limited extenuating circumstances may exist where an Authorized User must access CoPA IT Resources with a Privately Owned Device.

4. Definitions

4.1 Public Computers – Various computers available in public areas (i.e., libraries, schools, coffee shops) that many different individual users can access throughout the course of a day.

4.2 Privately Owned Devices – A non-Commonwealth owned device used by an Authorized User in which the Commonwealth has no responsibility for the procurement or maintenance of the asset, and it is solely the responsibility of the Authorized User.

This policy covers Privately Owned Devices that remotely access CoPA IT Resources. Privately Owned peripheral devices (i.e., monitors, keyboards, mouse, webcams, etc.) whether connecting to a Commonwealth issued device or a Privately Owned Device, do not require an IT Policy Waiver to be used by the Authorized User.

Note: external or portable electronic storage devices are not considered authorized peripheral devices.

5. Objective

- Provide requirements for Authorized Users to obtain the appropriate approvals for the temporary use of Privately Owned Devices to remotely access CoPA IT Resources.
- Provide requirements for Authorized Users to remotely access CoPA IT Resources with Privately Owned Devices.
- Define the appropriate connection method for Privately Owned Devices to remotely access CoPA IT Resources.

6. Policy

The use of Privately Owned Devices by Authorized Users to remotely access CoPA IT Resources is strictly prohibited. Only under the following extenuating circumstances and only for so long as the extenuating circumstance exists may a Privately Owned Device be utilized to remotely access COPA IT Resources:

- Pandemic, emergency, or disaster scenario requiring the Authorized User to have remote access to CoPA IT Resources in order for Commonwealth business to function; or
- Critical systems support during non-Commonwealth business hours requires the Authorized User to have remote access to CoPA IT Resources in order for Commonwealth business to function.

Under any other circumstances, the use of Privately Owned Devices by Authorized Users to remotely access CoPA IT Resources shall be in compliance with this ITP and only after an approved IT Policy Waiver is obtained by the Agency business area may the Authorized User use the Privately Owned Device to remotely access CoPA IT Resources. The waiver request shall include a timeline or estimated timeframe for the purchase of Commonwealth issued devices to negate the need for the use of Privately Owned Devices.

It is preferable that Commonwealth issued devices are used by Authorized Users for teleworking purposes. If Commonwealth issued devices are not available, the use of Privately Owned Devices must follow the requirements in this ITP, receive an approved IT Policy Waiver and a request to procure Commonwealth owned devices must be submitted.

For connectivity details, requests for approval to temporarily use Privately Owned Devices to remotely access CoPA IT Resources and steps to modify system configurations on Privately Owned Devices, follow the guidance in OPD-PLT012A *Connectivity Methods for Remotely Accessing Commonwealth IT Resources.*

Please note: Under no circumstances shall the Commonwealth be responsible to support and/or maintain the Authorized User's Privately Owned Device and approval to temporarily use the Privately Owned Device shall not imply such a responsibility. Further, the Authorized User shall not be entitled to nor shall the Authorized User receive assistance or reimbursement from the Commonwealth for configuration, installation, maintenance, repair, or replacement of the Authorized User's Privately Owned Devices.

Connecting Privately Owned Devices directly to CoPA IT Resources, including agency networks, is strictly prohibited.

When an Authorized User uses a Privately Owned Device to gain Remote Access to CoPA IT Resources or CoPA applications, the Authorized User must comply with the following criteria outlined below:

Connection to CoPA IT Resources shall be through Virtual Desktop Infrastructure (VDI).

Anti-Virus (AV) software shall be installed and kept current on the Privately Owned Device. For additional information, please refer to ITP-SEC001 *Enterprise Host Security Software Policy* for policy regarding anti-virus software.

Patches and security updates shall be kept current on the Privately Owned Device

in accordance with ITP-SYM006 *Commonwealth IT Resources Patching Policy*. For PCs with a Microsoft operating system, it is recommended that the Microsoft Windows Update feature be configured to automatically receive and install updates.

Authorized Users shall store and maintain all Commonwealth data on the CoPA managed system or service only. Commonwealth data shall never be saved locally to Privately Owned Device per Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Privately Owned Devices used to access CoPA IT Resources shall adhere to the same password requirements set forth by ITP-SEC007 *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*.

Authorized Users shall access data through the Privately Owned Device only in a manner that is in accordance and compliance with published IT policies and regulatory requirements mandated by your Agency.

Authorized Users shall report occurrences of cyber security incidents or data breaches on all Privately Owned Devices used to remotely access CoPA IT Resources in compliance with ITP-SEC024 *IT Security Incident Reporting Policy*.

Public Computers shall not be used to access CoPA IT Resources. Using a Public Computer to connect to a CoPA IT Resource poses a significant security risk. For instance, a third party may easily capture a user's logon credentials.

Privately Owned Printers shall not be used to print Commonwealth Data. Only Commonwealth issued printing devices shall be used to print Commonwealth Data.

A Privately Owned Device that is used to remotely access CoPA IT Resources may be seized and/or searched at the Commonwealth's discretion in connection with, but not limited to, a cyber security incident or breach, e-Discovery, Right-to-Know Law, or non-compliance with Commonwealth policies.

All electronic and hard copy records, data, and files created or maintained in connection with the performance of job duties are the property of the Commonwealth and are subject to applicable confidentiality and retention practices, regardless of where stored or maintained, and shall be subject to Right-to-Know Law as outlined in Management Directive 205.36 Amended *Right-To-Know Law Compliance*.

Privately Owned Devices used to remotely access CoPA IT Resources may be subject to access and inspection as outlined in Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Electronic information that is maintained or stored on a Privately Owned Device that remotely accesses IT Resources shall be collected for purposes of e-Discovery for litigation matters if a determination has been made by Agency Legal Counsel in compliance with ITP-INF009 *e-Discovery Technology Standards*.

Commonwealth issued and Privately Owned Mobile Communication Devices that are being used to conduct Commonwealth business must follow the guidance set in ITP-SEC035 *Mobile Device Security Policy*.

7. Responsibilities

7.1 Authorized Users shall:

- Sign a Telework Agreement if the Privately Owned Device is to be used for teleworking.
- Understand and comply with the responsibilities and requirements outlined in this policy.
- Validate and modify system configurations to comply with the criteria outlined in OPD-PLT012 *Connectivity Methods for Remotely Accessing Commonwealth IT Resources.*

7.2 Agencies shall:

- Create a plan and associated timeline to replace the use of Privately Owned Devices with Commonwealth owned devices.
- Submit a request to procure the appropriate Commonwealth owned devices for Authorized Users to replace the use of Privately Owned Devices.
- Coordinate with the appropriate OA/OIT submitter to facilitate the gathering of information and required artifacts for the submission of any IT Policy Waiver required under this Policy.
- After approval of the IT Policy Waiver is received, coordinate with OA/OIT to ensure the appropriate connectivity method is in place for the Authorized User's Privately Owned Device to remotely access CoPA IT Resources.

7.3 Office of Administration, Office for Information Technology (OA/OIT) shall:

- Coordinate with Agency to submit the IT Policy Waiver submission with required artifacts.
- Provide oversight, review, and approval of all IT Policy Waivers.
- After approval of IT Policy Waiver is received, coordinate with Agency to ensure the appropriate connectivity method is in place for Privately Owned Devices to remotely access CoPA IT Resources.

8. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal:

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- Management Directive 205.36 Amended *Right-to-Know Law Compliance*
- Management Directive 505.36 *Telework*
- OPD-PLT012A *Connectivity Methods for Remotely Accessing Commonwealth IT Resources*
- ITP-BUS002 *IT Investment Review Process*
- ITP-INF009 *e-Discovery Technology Standard*
- ITP-NET019 *Virtual Desktop Infrastructure*
- ITP-PLT002 *Multi-Function Equipment Management Policy*
- ITP-SEC001 *Enterprise Host Security Software Policy*
- ITP-SEC007 *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*

- ITP-SEC024 *IT Security Incident Reporting Policy*
- ITP-SYM006 *Commonwealth IT Resources Patching Policy*
- US-CERT Wireless Security - https://www.us-cert.gov/security-publications/using- wireless-technology-securely

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. Publication Version Control

It is the Authorized 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.

11. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

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

Version	Date	Purpose of Revision	Redline Link
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	
Revision	10/13/2021	• Updated Policy Title • Added Definitions and Objectives Sections • Updated extenuating circumstances • Updated Policy Section • Updated Exemption section to remove COPPAR reference • Created OPD-PLT012A to outline approval process, connectivity methods, equipment cost and system configuration changes to Privately Owned Devices	Revised ITP Policy Redline <10/13/2021>
Revision	10/18/2021	• Added reference to Privately Owned peripheral devices	Revised ITP Policy Redline <10/18/2021>