pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Virtual Private Network Standards

ITP Number ITP-SEC010	**Effective Date** June 22, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** September 2022

1. Purpose

This Information Technology Policy (ITP) provides guidance and standards to Commonwealth agencies to mitigate the risks associated with the transmission of sensitive information across networks when implementing Virtual Private Networks (VPNs) based on Internet Protocol Security (IPsec) or the Transport Layer Security (TLS) protocol.

2. Scope

This ITP applies to all departments, offices, 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.

Third-party vendors, licensors, contractors or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Policy

This ITP represents the minimum operational standards for network-based Internet Security Protocol (IPsec), Virtual Private Network (VPN) and Transport Layer Security (TLS) and VPN configurations between trusted and untrusted networks. The use of a VPN connection will be required for any access to the Commonwealth network from outside of the United States. Access to Microsoft Office 365 services (including email) and other cloud-based Commonwealth services from outside of the United States shall require an approved VPN connection.

The following are VPN integrated models that allow an agency to securely connect remote users and systems:

Gateway-to-Gateway VPN minimum policy requirements

The Gateway-to-Gateway VPN model protects communications between two specific networks, such as from one agency central office network to another, from an agency central office network to another internal agency branch office network, or between an agency's central offices to trusted business partners networks. Split-tunneling, which allows a Gateway to route traffic to a network outside of Gateway-to-Gateway VPN tunnel(s) at the same time, using the same or multiple physical network connections, is prohibited except for specific traffic as defined in OPD-SEC010A *Configurations for VPN Split-Tunneling*.

Network-to-network VPNs will use one of two methods: IPsec, which is password protected, or TLS, which provides encryption, authentication, and integrity verification of data by means of a digital certificate.

IPSec VPN Pre-shared Keys shall comply with the requirements defined in ITP-SEC007 *Minimum Standards for IDs, Passwords, and Multi-Factor Authentication*.

TLS VPN certificates requirements:

- The minimum certificates that can be signed is the SHA-2 signature algorithm, but it is recommended that the SHA-3 signature algorithm is utilized.

- No SSL versions are to be implemented on Commonwealth systems.

- Systems shall be configured to support the latest TLS version referenced in ITP-SEC031 *Encryption Standards.*

Host-to-Gateway VPN minimum policy requirements

This model protects communications between one or more individual Hosts and a specific network belonging to an agency. The host-to-gateway VPN model is most often used to allow hosts on unsecured networks, such as traveling employees and telecommuters, to gain access to internal organizational services. Split-tunneling, which allows a VPN user to access a public network (e.g., the internet) and a second VPN connection or WAN at the same time, using the same or multiple physical network connections, is prohibited except for specific traffic as defined in OPD-SEC010A *Configurations for VPN Split-Tunneling*. Local Area Network (LAN) access to local resources (printers, file shares) while connected to VPN is prohibited. VPN-Connected Host to VPN-Connected Host traffic (i.e. between connected VPN Clients) is prohibited.

Multi-factor authentication, as described in ITP-SEC039 *Keystone Login and Identity Proofing*, shall be utilized for a Host-to-Gateway VPN.

Agencies are to comply with product standards as described in this document and ITP-SEC031 - *Encryption Standards*.

Session Length Requirements

The Office of Administration has configured an Enterprise-wide Host-to-Gateway maximum VPN session length as defined in OPD-SEC010A *Configurations for VPN Split-Tunneling and Host-to-Gateway Session Length* to meet known compliance requirements.

While connected to VPN, the remaining session time prior to the VPN session automatically terminating is continuously displayed in the VPN client on the main window. After this time expires, users must reauthenticate.

VPN Remote Access Multi-Factor requirements

Multi-factor authentication requires users to provide at least two proofs of their identity, which increases security for access to Commonwealth resources. It reduces the risk that business or personal information stored in administrative systems will be compromised. The following chart below identifies the minimum multi-factor authentication methods required for remote access to Commonwealth resources.

Enterprise Systems	Access Method
Current Telecom Service Provider Systems	Management console / Portal
Commonwealth Systems	Remote VPN connection
Enterprise Roles	**Access Method**
Enterprise CWOPA Active Directory administrators	Remote VPN connection

VPN Remote Access Control endpoint checks:
VPN elements of an endpoint check will be enforced to check for current anti-virus software and operating system service pack levels before the remote user will be allowed access to the network.

The following are requirements related to all agency managed or enterprise remote access systems.

Desktop/Laptop Operating Systems, Internet Browsers, and Mobile Devices:

- Hardware ownership may be checked upon connection attempt.
- Commonwealth-issued desktop or laptop operating systems that are categorized as Current and Contain status, as documented in ITP-PLT017 *Desktop and Laptop Operating Systems Standards*, are allowed remote access.
- Any Commonwealth-issued desktop or laptop operating system categorized as Retired or not listed in ITP-PLT017 are not allowed remote access.
- Non-Commonwealth electronic devices that have been approved for Commonwealth business and adhere to ITP-PLT012 *Use of Electronic Devices to Access IT Resources* are allowed remote access.
- Commonwealth-issued mobile devices that adhere to ITP-SEC035 *Mobile Device Security Policy* are allowed remote access.

Endpoint Security and Patches:
The following link contains a list of supported anti-virus applications for endpoint checks: https://itcentral.pa.gov/Security/Pages/Services.aspx (Protection/Endpoint) (*CWOPA access only*). In addition,

- Anti-virus definitions need to comply within a maximum of ten (10) definition file versions from the vendor's latest release.
- Desktop and laptop operating systems need to follow ITP-PLT017 *Desktop and Laptop Operating System Standards*.
- Internet browsers need to follow ITP-SFT006 *Internet Browser Policy*.

4. Standards

CURRENT

These technologies meet the requirements of the current architecture and are recommended for use.

Technology	Platforms	Category	Technology Classification
Current Telecom Service/Product Offerings	Current Telecom Service/Product Offerings	VPN	Current

EMERGING/RESEARCH

These technologies have the potential to become current standards and are to be used only in pilot or test environments where they can be evaluated. Use of these technologies requires approval of a waiver request.

Technology	Platforms	Category	Technology Classification
--	--	--	--

5. Responsibilities

5.1 Agencies shall comply with the requirements as outlined in this ITP.

5.2 Third-party vendors, licensors, contractors, or suppliers shall:

- Provide access to the third-party vendor's, licensor's, contractor's or suppliers's networks and connected systems over Virtual Private Network (VPN).
- Ensure VPN connection is utilized for any access to the Commonwealth network from external sources.

6. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

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*
- OPD-SEC010A – *Configurations for VPN Split-Tunneling and Host-to-Gateway Session Length*
- ITP-ACC001 *Information Technology Digital Accessibilty Policy*
- ITP-PLT012 – *Use of Privately Owned PCs To Access CoPA Resources*
- ITP-PLT017 – *Desktop and Laptop Operating System Standards*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC007 - *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*
- ITP-SEC031 – *Encryption Standards*
- ITP-SEC035 – *Mobile Device Security Policy*
- ITP-SEC039 – *Keystone Login and Identity Proofing*
- ITP-SFT006 – *Internet Browser Policy*
- NIST SP 800-46 Rev. 2 - *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- NIST SP 800-52 Rev. 2 - *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- NIST SP 800-77 Rev. 1 - *Guide to IPsec VPNs*
- NIST SP 800-113 - *Guide to SSL VPNs*

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. 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.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy 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. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	06/22/2006	Base Document	N/A
Revision	08/01/2012	Align to the changes in security under the current telecommunications contract. Differentiate between supported operating systems for Dial-Up connections and Broadband connections. Added grace period for host-checks. Clarified split-tunneling definition. Modified DAT file definition.	N/A
Revision	12/05/2012	Incorporated STD-SEC010A - Product Standards for Virtual Private Networks and clarifying language concerning two-factor authentication methods.	N/A
Revision	12/05/2013	ITP Refresh – converted ITB to ITP format	N/A
Revision	03/17/2014	Removed Windows XP from supported list of operating systems. Added Windows 8/8.1 to supported list of operating systems.	N/A
Revision	03/31/2016	• Added Definitions section • Removed Contain and Retire categories in Standards sections • Expanded Policy Section to include: o Network-to-network methods o IPsec VPN password requirements o TLS VPN certificate requirements o Added language to not use SSL and removed SSL references o Expanded endpoint check criteria language ▪ added Internet Browser ▪ added Service Pack Levels o Updated vendor reference page URLs o Added Client-side Cache Cleaner language • Added references ITP-APP035, ITP-PLT017, ITP-SEC035	N/A
Revision	04/08/2018	• Updated ITP references • Removed Objectives section • VPN requirement for outside US to access Commonwealth cloud platforms • Moved Definitions to online Policy Glossary • Added link to Endpoint A/V applications list • Revised language throughout for clarity	N/A
Revision	12/04/2019	• Removed security token / digital certification information • Moved terms to online glossary and linked terms throughout	Revised IT Policy Redline <12/04/2019>
Revision	06/23/2020	• Removed browser check • Added OPD-SEC010A for Split Tunneling • Added Hardware Ownership check. • Added prohibition on local LAN access. • Added prohibition on Connected Host to Connected Host traffic • Removed Client-Side Cache Cleaner	Revised IT Policy Redline <06/23/2020>
Revision	05/13/2021	• Added Split Tunneling to Gateway-to-Gateway (OPD updated to match) • Removed reference to Internet Browser check and policy.	Revised IT Policy Redline <05/13/2021>

Revision	07/12/2021	• Added Third-party vendors to Scope and Responsibilities Section • Added Responsibilities Section	Revised IT Policy Redline <07/12/2021>
Revision	09/20/2021	• Added session length requirement to Purpose/Policy. • Updated Scope and Responsibilities section. • Updated references and links	Revised IT Policy Redline <09/20/2021>