

# Information Technology Policy

## *Virtual Private Networks*

<b>Number</b> ITP-SEC010	<b>Effective Date</b> June 22, 2006
<b>Category</b> Security	<b>Supersedes</b> None
<b>Contact</b> <a href="mailto:RA-ITCentral@pa.gov">RA-ITCentral@pa.gov</a>	<b>Scheduled Review</b> January 2024

### 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 offices, departments, boards, commissions and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

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 [IPsec](#), and [TLS](#) VPN configurations between trusted and untrusted networks. The use of an approved VPN connection will be required for any access to the Commonwealth network from outside of the United States; this includes access to Microsoft Office 365 services (including email) and other cloud-based Commonwealth services from outside of the United States.. Agencies shall comply with [ITP-SEC000, Information Security Policy](#) and submit an [IT Policy Waiver](#) request for all OCONUS access requests. Please note that approval is not guaranteed. Use of alternative connectivity such as Virtual Desktop Infrastructure ([VDI](#)) is strongly encouraged over VPN to further limit risk. Agencies shall refer to [STD-SEC010B, Virtual Private Network Standards](#) (Commonwealth Authorized Access Only) for a listing of current VPN standards.

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 is prohibited except for specific traffic as defined in *OPD-SEC010A, Configurations for VPN Split-Tunneling* (Commonwealth Authorized Access Only).

Network-to-network VPNs shall use one of two methods: IPsec, which is password protected, or TLS, which uses 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 Secure Hash Algorithm 2 (SHA-2), but it is recommended that SHA-3 signature algorithm is utilized.
- All Secure Sockets Layer (SSL) versions are strictly prohibited.
- Systems shall be configured to support the at least the minimum 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 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-SEC007 - Minimum Standards for IDs, Passwords, Sessions and Multi-Factor Authentication](#), 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, Office for Information Technology (OA/OIT) 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. All remote access VPN logins require multi-factor authentication.

## 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](#), shall be allowed remote access.
- Any Commonwealth-issued desktop or laptop operating system categorized as Retired or not listed in [ITP-PLT017](#) shall not be 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](#) shall be allowed remote access.
- Commonwealth-issued mobile devices that adhere to [ITP-SEC035, Mobile Device Security Policy](#) shall be allowed remote access.

### Endpoint Security and Patches:

A list of supported anti-virus applications for endpoint checks can be found on the [IT Central Security Services Page](#) under Protection/Endpoint (*Commonwealth access only*). In addition:

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

## 4. Responsibilities

### 4.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

### 4.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

#### 4.3 Third-party vendors, licensors, contractors, or suppliers shall:

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

### 5. 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 (Commonwealth Authorized Access Only)*
- *STD-SEC010B, Virtual Private Network Standards (Commonwealth Authorized Access Only)*
- [\*ITP-ACC001, Information Technology Digital Accessibility 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-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\*](#)

### 6. Authority

[\*Executive Order 2016-06, Enterprise Information Technology Governance\*](#)

### 7. 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 shall be directed to [RA-ITCentral@pa.gov](mailto:RA-ITCentral@pa.gov).

## 8. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to [ITP-BUS004, IT Policy Waiver Review Process](#) for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to Commonwealth users only.

Version	Date	Purpose of Revision	Redline Link
Original		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	<ul style="list-style-type: none"> <li>• Added Definitions section</li> <li>• Removed Contain and Retire categories in Standards sections</li> <li>• Expanded Policy Section to include: <ul style="list-style-type: none"> <li>○ Network-to-network methods</li> <li>○ IPsec VPN password requirements</li> <li>○ TLS VPN certificate requirements</li> <li>○ Added language to not use SSL and removed SSL references</li> <li>○ Expanded endpoint check criteria language <ul style="list-style-type: none"> <li>▪ added Internet Browser</li> <li>▪ added Service Pack Levels</li> </ul> </li> <li>○ Updated vendor reference page URLs</li> <li>○ Added Client-side Cache Cleaner language</li> </ul> </li> </ul> <p>Added references ITP-APP035, ITP-PLT017, ITP-SEC035</p>	N/A
Revision	04/08/2018	<ul style="list-style-type: none"> <li>• Updated ITP references</li> <li>• Removed Objectives section</li> <li>• VPN requirement for outside US to access Commonwealth cloud platforms</li> <li>• Moved Definitions to online Policy Glossary</li> <li>• Added link to Endpoint A/V applications list</li> <li>• Revised language throughout for clarity</li> </ul>	N/A
Revision	12/04/2019	<ul style="list-style-type: none"> <li>• Removed security token / digital certification information</li> <li>• Moved terms to online glossary and linked terms throughout</li> </ul>	N/A
Revision	06/23/2020	<ul style="list-style-type: none"> <li>• Removed browser check</li> <li>• Added OPD-SEC010A for Split Tunneling</li> <li>• Added Hardware Ownership check.</li> </ul>	N/A

Version	Date	Purpose of Revision	Redline Link
		<ul style="list-style-type: none"> <li>Added prohibition on local LAN access.</li> <li>Added prohibition on Connected Host to Connected Host traffic</li> <li>Removed Client-Side Cache Cleaner</li> </ul>	
Revision	05/13/2021	<ul style="list-style-type: none"> <li>Added Split Tunneling to Gateway-to-Gateway (OPD updated to match)</li> <li>Removed reference to Internet Browser check and policy.</li> </ul>	N/A
Revision	07/12/2021	<ul style="list-style-type: none"> <li>Added Third-party vendors to Scope and Responsibilities Section</li> <li>Added Responsibilities Section</li> </ul>	N/A
Revision	09/20/2021	<ul style="list-style-type: none"> <li>Added session length requirement to Purpose/Policy.</li> <li>Updated Scope and Responsibilities section.</li> <li>Updated references and links</li> </ul>	N/A
Revision	01/20/23	<ul style="list-style-type: none"> <li>Updated ITP title.</li> <li>Created STD-SEC010B and moved standards charts to STD. Added references to new standards doc throughout ITP.</li> <li>Updated scope based upon connection to Commonwealth network.</li> <li>Added language regarding ITP-SEC000/OCONUS Access and waiver requirement.</li> <li>Removed chart under VPN Remote access MFA requirements and added policy requirement language.</li> <li>Updated reference to IT Central under Endpoint Security and Updates.</li> </ul>	<a href="#">Revised IT Policy Redline &lt;01/20/2023&gt;</a>