Information Technology Policy
Virtual Private Networks

Number
ITP-SEC010

Effective Date
June 22, 2006

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
September 2024

1. Purpose

This Information Technology Policy (ITP) establishes the policy, responsibilities, and procedures for mitigation of 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 (Service Organizations) 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 is required for any access to the Commonwealth's IT resources 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 access only) for a listing of current VPN standards.

Agencies shall utilize the Gateway-to-Gateway or Host-to-Gateway (inbound) VPN integrated models to facilitate a secure connection between remote users and/or

systems.

3.1 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 protocols: IPsec, as a digital certificate (preferred) or pre-shared key, 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*.

Systems shall be configured to support at least the minimum configurations (ciphers, protocols, and signing) referenced in *ITP-SEC031, Encryption Standards*.

3.2 Host-to-Gateway (Inbound) 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 (Commonwealth authorized access only)*. 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 the standards as described in this document and *ITP-SEC031, Encryption Standards*.

3.3 Host-to-Gateway (Outbound) VPN Policy Restriction

Commonwealth Hosts are prohibited from being configured or utilizing any non-commonwealth VPN clients to individually connect and access any non-commonwealth IT resources (including networks). This includes host VPN connections to Business Partners, Federal partners, and Service Organizations.

In instances where agencies require this type of secure collaboration with an external partner, the Gateway-to-Gateway VPN model is required.

3.4 Session Length Requirements

The Office of Administration, Office for Information Technology (OA/IT) 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 (Commonwealth authorized access only)* to meet 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.

3.5 VPN Remote Access Multi-Factor Requirements

All remote access VPN logins require multi-factor authentication (MFA). MFA requires users to provide at least two proofs of their identity, which increases security for access to Commonwealth IT resources. It reduces the risk that business or personal information stored in administrative systems will be compromised.

3.6 VPN Remote Access Control Endpoint Checks

VPN elements of an endpoint check are 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 requirements related to all agency managed or enterprise remote access systems and technologies (Desktop/Laptop Operating Systems and Mobile Devices) shall be met:

- Commonwealth-issued desktops or laptop operating systems shall be compliant with Current and Contain standards per *ITP-PLT017, Desktop and Laptop Operating Systems Standards*.
- Commonwealth-issued mobile devices shall comply with *ITP-SEC035, Mobile Device Security Policy* and are authorized for remote access.
- Non-Commonwealth electronic devices shall be compliant with *ITP-PLT012, Use of Privately Owned Devices to Access IT Resources* and shall have been approved for such use through a current approved IT Policy Waiver.

Any Commonwealth-issued desktop or laptop operating system categorized as Retired or not listed in *ITP-PLT017, Desktop and Laptop Operating Systems Standards* is prohibited from being utilized for remote access.

Hardware ownership may be checked upon connection attempt.

A list of supported anti-virus applications for endpoint checks can be found on the IT Central Security Services Page under Protection/Endpoint (*Commonwealth authorized 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*.

3.7 VPN Configurations for Service Organizations

Service Organizations shall refer to *OPD-SEC010C, Site to Site VPN Configurations for Service Organizations* when determining the configurations for an appropriate VPN solution within their environment for systems which host or transmit Commonwealth Data.

4. Responsibilities

4.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

4.2 OA/IT shall:

Comply with the requirements as outlined in this ITP.

4.3 Service Organizations shall:

- Provide access to the Service Organization's networks and connected systems over VPN.
- Ensure VPN connection is utilized for any access to the Commonwealth network from external sources and in alignment with specifications outlined in *OPD-SEC010C, Site to Site VPN Configurations for Service Organizations*.

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)*
- *OPD-SEC010C, Site to Site VPN Configurations for Service Organizations (Commonwealth authorized access only, available by request, RA-ITCentral@pa.gov)*
- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *ITP-PLT012, Use of Privately Owned Devices to Access IT 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.

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	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:
		  ○ Network-to-network methods
		  ○ IPsec VPN password requirements
		  ○ TLS VPN certificate requirements
		  ○ Added language to not use SSL and removed SSL references
		  ○ Expanded endpoint check criteria language
		  ▪ added Internet Browser
		  ▪ added Service Pack Levels
		  ○ Updated vendor reference page URLs
		  ○ 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	N/A

Version	Date	Purpose of Revision	Redline Link
		• Added link to Endpoint A/V applications list • Revised language throughout for clarity	
Revision	12/04/2019	• Removed security token / digital certification information • Moved terms to online glossary and linked terms throughout	N/A
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	N/A
Revision	05/13/2021	• Added Split Tunneling to Gateway-to-Gateway (OPD updated to match) • Removed reference to Internet Browser check and policy.	N/A
Revision	07/12/2021	• Added Third-party vendors to Scope and Responsibilities Section • Added Responsibilities Section	N/A
Revision	09/20/2021	• Added session length requirement to Purpose/Policy. • Updated Scope and Responsibilities section. • Updated references and links	N/A
Revision	01/20/23	• Updated ITP title. • Created STD-SEC010B and moved standards charts to STD. Added references to new standards doc throughout ITP. • Updated scope based upon connection to Commonwealth network. • Added language regarding ITP-SEC000/OCONUS Access and waiver requirement. • Removed chart under VPN Remote access MFA requirements and added policy requirement language. • Updated reference to IT Central under Endpoint Security and Updates.	N/A
Revision	09/26/23	• Replaced network with IT resource where appropriate • Added link to STD-SEC010B • Added section numbers to policy language to define separate policy sections • Technical details on VPN TLS configurations removed and statement referring to ITP-SEC031 updated. • Added additional references to OPD-SEC010A where appropriate • Updated name of PLT012 consistent with policy title • Added section 3.7 VPN Configurations for Service Organizations and accompanying based policy language with supporting document reference. • Added reference to OPD-SEC010C Site to Site VPN Configurations for Service Organizations • Updated Responsibilities under 4.3 to include alignment to OPD-SEC010C for Service Organizations • Streamlining of section 3.3 VPN Remote Access Control Endpoint Checks to clean up policy requirements • Added policy restriction around host to gateway outbound and accompanying policy language.	Revised IT Policy Redline <09/26/2023>