Information Technology Policy

Commonwealth Metropolitan Area Network (MAN) and Internet Access

Number
ITP-NET018

Effective Date
August 16, 2007

Category
Network

Supersedes
All Prior Versions

Contact
RA-ITCentral@pa.gov

Scheduled Review
July 2023

1. Purpose

Establishes an enterprise-wide policy for the connection, software, technology, and central administration of the Commonwealth's connectivity to the Internet.

2. Scope

This Information Technology Policy (ITP) applies to all entities on or connected to the Commonwealth Enterprise Network including all offices, departments, boards, commissions, councils, or any other organization (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth as outlined in the Responsibilities Section.

3. Definitions

3.1 **Commonwealth Point of Presence (CPOP):** Locations that provide access to the enterprise network backbone, which is comprised of COPANET and any extended backbone delivered by enterprise telecommunications providers.

3.2 **Direct Internet Access (DIA):** Any network service that delivers connectivity to the Internet without the use of the Commonwealth's Enterprise Network and/or Enterprise Perimeter Security solution.

3.3 **Managed Device:** A device that is configured and monitored via graphical user interface, command line interface, simple network management protocol, syslog, and/or similar methods with a periodic review of the logs and device status by the organization maintaining it

3.4 **Metropolitan Area Network (MAN):** The network that interconnects agencies or entities with computer resources within the Commonwealth of Pennsylvania.

3.5 **Software-Defined Wide Area Network (SD-WAN):** Solutions that provide a replacement for traditional wide area network (WAN) routers and are agnostic to WAN transport technologies. Provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

3.6 **Virtual Routing and Forwarding (VRF):** Technology that allows for secure logical separation of traffic and maintains separate routing and forwarding tables to segment the traffic between each instance within a device.

4. Policy

4.1 General

Agencies shall access the Internet through the Commonwealth MAN.

The Office of Administration, Office for Information Technology (OA/OIT) is responsible for the following:

- Serve as primary point of contact for Internet access through the Commonwealth's Network, as well as the Commonwealth's point of contact with the Commonwealth's Internet access providers.
- Oversee development, implementation, and operation of a plan for interagency security.
- Direct security assessments of agency Information Technology (IT) resources that connect to the MAN and audit agencies to ensure compliance as outlined in ITP-SEC023, *Information Technology Security Assessment and Testing Policy*.
- Disconnect or otherwise render inaccessible any network that poses a security risk to the Commonwealth's enterprise network until it is determined that the risk has been adequately mitigated.
- Maintain centralized registration, management, and distribution of Internet protocol (IP) addresses. Refer to ITP-NET004 *Internet Protocol Address Standards*.
- Maintain domain naming standards, registration, management, desktop, and server configuration. Refer to ITP-NET005 *Commonwealth Domain Naming Standards (DNS) and Configuration*.

Each Commonwealth agency is responsible for the following:

- Develop policies and procedures to ensure security of its IT resources. Information disseminated over the Internet shall be approved in accordance with agency and Commonwealth policies prior to its release.
- Perform self-audit of compliance with applicable ITPs including conducting annual risk assessments.
- Evaluate and report Cyber Security Incidents according to ITP-SEC024, *IT Security Incident Reporting Policy*.
- Cooperate and collaborate with the Office of Administration, Enterprise Information Security Office (OA/EISO) when responding to Cyber Security Incidents, including investigation, containment, eradication, recovery, and post-incident analysis.

- Provide the Commonwealth's Chief Information Security Officer with an agency primary and secondary point of contact for cyber security incident reporting and handling. The primary point of contact shall be the agency Information Security Officer (ISO). Agencies may choose who will serve as the secondary point of contact. Refer to ITP-SEC016, Commonwealth of Pennsylvania - Information Security Officer Policy.

4.2 DIA and SD-WAN Technologies

Agencies or providers utilizing DIA and SD-WAN technologies with connectivity back to the Commonwealth enterprise network must deploy and maintain solutions that adhere to the following requirements:

- Provide the Office of Administration, Enterprise Technology Services Office (OA/ETSO) and OA/EISO with accurate network diagram(s) for review and approval prior to deployment and/or service redesign via the enterprise change management process. These diagram(s) must contain complete IP network information showing locations and connectivity to the agency, public, managed vendor point of presence, networks, and any network and security control devices that govern the traffic.
- Maintain up-to-date diagrams for audit and approval. The designs including these diagrams must be provided to OA/OIT for audit and approval via the enterprise change management process.
- Provide access for OA/OIT to review SD-WAN device configurations.
- Provide access for OA/OIT to review traffic and configuration change logs.
- Traffic logs must include:
    - Uniquely identifying client device and/or user information.
    - Device change logs must include:
        - UserID (must adhere to ITP-SEC007 *Minimum Standards for IDs, Passwords and Multi-Factor Authentication*)
        - Time of login
        - Modification performed (include customer change request/ticket number in comment field).
- Follow Cyber Security Incident reporting procedures as defined in ITP-SEC024, *IT Security Incident Reporting Policy*.
- Utilize only Managed Devices for delivery of the services.
- Provide properly configured and activated intrusion detection and prevention services.
- Provide content filtering capability and properly configure content filter in compliance with ITP-SEC003, *Enterprise Content Filtering Standard.*
- DIA Networks shall only be permitted in conjunction with SD-WAN services.
- Prohibit all cross-VRF traffic except where explicitly allowed by the enterprise ITP policies.

4.3 Connectivity Requirements

Agencies or providers deploying or operating DIA connections with connectivity to the Commonwealth must deploy solutions that adhere to the following requirements:

- All devices connecting to the Commonwealth must be maintained on dedicated VRF network(s) at the remote location.
- A site-to-site tunnel must be established from the SD-WAN device at the DIA location to a head-end device located within a CPOP.
- The CPOP-located head-end device may connect the dedicated VRF network(s) to the appropriate corresponding agency, MAN, BP, or VRF.
- Devices inside any Commonwealth VRF are prohibited from direct Internet connectivity for any traffic via the DIA circuit or any other locally provided Internet connection without explicit OA permission. Any traffic for the Commonwealth VRF that is not explicitly permitted by OA to use the DIA must traverse the site-to-site tunnel and exit to the Internet through the agency and Commonwealth enterprise networks. Requests for DIA routing of traffic from this VRF must be submitted via the policy waiver process. Refer to Section 9 for guidance.
- All configurations must comply with the provisions set forth in ITP-SEC010 *Virtual Private Network Standards* and OPD-SEC010A *Configurations for VPN Split-Tunneling* (authorized Commonwealth personnel only).

4.4 Agency Direct Internet Access

Agencies may utilize DIA for devices that do not require any connectivity to the Commonwealth enterprise network (e.g., credit card readers whose only connectivity is with the credit processing service). Agencies or providers deploying services permitted under this use-case must deploy solutions that adhere to the following requirements:

- Prohibit cross-connection between Commonwealth devices and the devices using this service.
- Prohibit all connectivity between this network and any other local networks, including but not limited to any public Internet access subnets.

5. Responsibilities

5.1 **OA/OIT** operates and maintains the MAN and is the primary point of contact for all operations relating to the MAN.

5.2 **Commonwealth Agencies** shall adhere to the guidance set forth in this policy and shall obtain appropriate approval for all deviations from this policy. Agencies shall consult with OA prior to integrating any IT resources (such as software and hardware) into the MAN.

5.3 **Third-party vendors, licensors, contractors, or suppliers** shall comply with the requirements as outlined in this ITP that are applicable to the products or services they are providing to the Commonwealth. If the products or services being provided by the third-party vendor, licensor, contractor, or supplier do not fall within the scope of this ITP, compliance is implied. If the third-party vendor, licensor, contractor, or supplier subsequently deploys products or services that fall within the scope of this ITP in the future, compliance with the policy is required.

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
- Management Directive 505.7 *Personnel Rules (Section 22.1a)*
- ITP-NET004 *Internet Protocol Address Standards*
- ITP-NET005 *Commonwealth External and Internal Domain Name Services (DNS)*
- ITP-NET017 *Network Timing Protocol*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC001 *Enterprise Host Security Software Policy*
- ITP-SEC002 *Internet Accessible Proxy Servers and Services*
- ITP-SEC003 *Enterprise Content Filtering Standard*
- ITP-SEC007 *Minimum Standards for IDs, Passwords and Multi-Factor Authentication*
- ITP-SEC010 *Virtual Private Network Standards*
- OPD-SEC010A *Configurations for VPN Split-Tunneling* (authorized Commonwealth personnel only)
- ITP-SEC016 *Commonwealth of Pennsylvania - Information Security Officer Policy*
- ITP-SEC024 *IT Security Incident Reporting Policy*
- ITP-SEC031 *Encryption Standards for Data in Transit*
- ITP-SEC034 *Enterprise Firewall Rule Set*

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 shall 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 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 CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	08/16/2007	Base Document	N/A
Revision	12/20/2010	ITP Refresh	N/A
Revision	09/13/2019	ITP Reformat Added Definitions Added Direct Internet Access with SD-WAN technology guidance Updated References Removed unnecessary language throughout	N/A
Revision	07/29/2022	ITP Refresh Scope updated to include any entity connecting to the Commonwealth Network (including third parties) Updated definition for Metropolitan Area Network Updated OIT and Agency responsibilities related to Commonwealth MAN Updated requirements related to DIA and SD-WAN Added new standard language to responsibilities for third parties	Revised IT Policy Redline <07/29/2022>