pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Commonwealth Metropolitan Area Network (MAN) and Internet Access

ITP Number ITP-NET018	**Effective Date** August 16, 2007
Category Network	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** September 2020

1. Purpose

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

2. Scope

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

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 (EPS) solution.

3.3 Metropolitan Area Network (MAN): A network that interconnects users with computer resources in a geographic area or region such as the Commonwealth of Pennsylvania.

3.4 Software-Defined Wide Area Network (SD-WAN): Solutions that provide a replacement for traditional 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.

3.5 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.

3.6 Managed Device: A device that is configured and monitored via Graphical User Interface (GUI), Command Line Interface (CLI), Simple Network Management Protocol (SNMP), syslog, and/or similar methods with a periodic review of the logs and device status by the organization maintaining it.

4. Policy

4.1 General

Agencies are to access the internet through the Commonwealth Metropolitan Area Network (MAN). The Office of Administration (OA) is responsible for the following:

- Serve as primary point of contact for internet access through the Commonwealth's MAN, as well as the Commonwealth's point of contact with the Commonwealth's internet access provider.
- Oversee development and implementation of a plan for interagency MAN security.
- Direct security assessments of agency IT resources that connect to the MAN and audit agencies to ensure compliance.
- Maintain centralized registration, management, and distribution of internet protocol (IP) addresses. Refer to ITP-NET004 *Internet Protocol Address Standards*.
- Maintain domain naming standards (DNS), 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 is to be approved in accordance with agency policy prior to its release.
- Agencies are to evaluate cyber security incidents according to ITP-SEC024 *IT Security Incident Reporting Policy*.
- Agencies are to cooperate and collaborate with the Office of Administration, Enterprise Information Security Office (OA/EISO) when responding to cyber security incidents, which include investigation, containment, eradication, recovery and post-incident analysis.
- Agencies are to provide the Commonwealth's Chief Information Security Officer (CISO) with a primary and secondary point of contact for cyber security incident reporting and handling. The agency Information Security Officer (ISO) is to be the primary point of contact. Agencies are to provide the appropriate contact for those points of contact. Refer to ITP-SEC016 *Commonwealth of Pennsylvania - Information Security Officer Policy* for further guidance.

4.2 Direct Internet Access (DIA) and Software-Defined Wide Area Network (SD-WAN) Technologies

Agencies and/or providers wishing to utilize DIA and SD-WAN technologies with connectivity back to the commonwealth enterprise network must deploy solutions that adhere to the following requirements:

- Provide the 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 (POP), networks, and any network and security control devices that govern the traffic.

- Maintain updates to the diagrams for audit and approval. The designs including these artifacts must be provided to OA for audit and approval via the enterprise change management process.
- Provide access for OA to review SD-WAN device configurations.
- Provide access for OA 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 (login policies 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 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 (IDPS).
- Provide content filtering capability (Refer to ITP-SEC003 *Enterprise Security Auditing and Monitoring Internet Access Control and Content Filtering Standard* for guidance).
- Properly configure content filter in compliance with ITP polices.
- Prohibit all cross-Virtual Routing and Forwarding (VRF) traffic except where explicitly allowed by the enterprise ITP policies.

4.3 Connectivity Requirements

Agencies and/or providers deploying 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 Commonwealth Point of Presence (CPOP).
- The CPOP-located head-end device may connect the dedicated VRF network(s) to the appropriate corresponding agency, MAN, BP, or VRF.
- Devices within a VRF must not be permitted to have 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 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.

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 and/or providers deploying services

permitted under this use-case must deploy solutions that adhere to the following requirements:

- Prohibit cross-connection between commonwealth enterprise 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 The **Office of Administration (OA)** operates and maintains the Commonwealth Metropolitan Access Network (MAN) and is the primary point of contact for all operations relating to the MAN.

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

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 *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-SEC001 *Enterprise Host Security Software Policy*
- ITP-SEC002 *Internet Accessible Proxy Servers and Services*
- ITP-SEC003 *Enterprise Security Auditing and Monitoring Internet Access Control and Content Filtering Standard*
- ITP-SEC007 *Minimum Standards for IDs, Passwords and Multi-Factor Authentication*
- 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 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	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	Revised IT Policy Redline <09/13/2019>