Information Technology Policy
Telecommunications Services for Commonwealth Business Partners

Number		**Effective Date**	
ITP-NET008		June 18, 2004	
Category		**Supersedes**	
Network		All Prior Versions	
Contact		**Scheduled Review**	
RA-ITCentral@pa.gov		June 2023	

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish an enterprise-wide policy for Commonwealth business partners to provision voice and data services for the exchange of information with the Commonwealth.

2. Scope

This 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, suppliers or business partners (hereinafter referred to as "business partners'") shall meet the policy requirements of this ITP as outlined in the Responsibility Section.

3. Policy

This policy supports the exchange of information between agencies and their business partners through the provisioning of voice and data services.

Business partners shall be sponsored by agencies. A description of the business partner's service requirements shall be submitted to the Office of Administration/Office for Information Technology (OA/OIT) at ens@pa.gov for review and approval. Agencies shall expect that OA/OIT will periodically audit any existing business partner connections in an effort to obtain or update required information.

All services provided to a business partner shall be used solely for the business partner's support of its business activities associated with the Commonwealth as agreed upon between the sponsoring agency and business partner.

Routing: Static IP addresses are the standard. If the Border Gateway Protocol (BGP) is required, an [IT Policy waiver](#) is required by the sponsoring agency to validate requirements for this connectivity request.

A new service request is always required when engaging new Business Partner connections. This permits Enterprise Network Operation Section (ENOS) to review bandwidth requirements that may impact the OA MAN to OA Business Partner network connectivity.

Telecommunications Services Provided for Business Partners

All voice and data services, with the exception of the Commonwealth's Internet Connection, are available to business partners. Business partners shall procure their own Internet connection through the Commonwealth's Telecommunications Service Provider (TSP) or the provider of their choice.

All business partners, for security purposes, shall access the Commonwealth data network through the designated business partner network provided by the Commonwealth, and will be logically routed by Commonwealth-assigned Internet protocol addresses to the enterprise business partner routers and firewalls. Business partner firewall additions, changes, and deletions are subject to standard intervals per the ITSM Change Management process and shall be submitted by authorized agency security personnel using the ITSM Service Request process.

Business partner routing additions, changes, and deletions require a minimum seven-business day turnaround and shall be submitted by authorized agency network personnel to ENOS (ens@pa.gov) through a service request process. ENOS will review the request and assign to the appropriate vendor support network management.

Emergency requests for both security and routing will be handled on a case-by-case basis.

The Commonwealth does not automatically provide business partner redundancy. It is an option that can be ordered and provisioned through the requesting agency and the Commonwealth's service provider.

Business Partner-to-Business Partner Communications

Business partner-to-business partner communications are not recommended, and use shall be limited to Commonwealth-only business. Commonwealth agencies shall submit a written request for direct business partner-to-business partner communications to ens@pa.gov for review and approval. The request shall be based on specific requirements to conduct Commonwealth-only business.

Business partners participating in business partner-to-business partner communications shall use ENOS provided network addressing that is not routable to the Internet.

Devices equipped with dual or multiple network interface adapters shall maintain non-routable network addressing assigned by the Commonwealth.

Business Partner Co-Location

Agencies considering sponsoring a business partner connection through a Commonwealth business partner Co-Location facility shall engage ENOS, ens@pa.gov, by means of a service request at the onset or as early as possible to provide or collaborate on requirement, contractual, and governance details regarding the prospective relationship.

A business partner may order intrastate or interstate data service from any local exchange carrier of its choice. Information regarding local carrier connectivity is available by contacting ENOS. The service shall terminate and enter through the OA/OIT-established business partner co-location networks. Prior to placing orders for data services, the business partner and sponsoring agency shall confer with ENOS regarding cabling infrastructure at the co-location and its facilities.

Business Partner site to site VPN

Business partner VPN connectivity is governed by the following ITPs:

- [ITP-NET019 Virtual Desktop Infrastructure](#)

- [ITP-SEC010 Virtual Private Network Standards](#)

- [ITP-SEC034 Enterprise Firewall Rule Set](#)

- [ITP-SEC031 Encryption Standards](#)

Business partners may supply and manage their own router(s) and related equipment (encryption devices, modems, etc.) at any or all business partner co- location facilities.

Business partner or carrier addressing is permitted in the case of direct serial/WAN interface connections on the business partner co-location routers.

Business Partner Security and Standards

The Commonwealth will not provide network security for business partners connected to the Commonwealth's business partner network. Network security is the sole responsibility of the business partner.

It is recommended that business partners implement appropriate industry standard security solutions, policies and procedures to ensure enterprise security compliancy. Firewalls, access control lists on routers, and anti-virus protection solutions are considered minimum required security standards. Additional security measures that business partners deem prudent are also acceptable and recommended.

Business partners are expected to prevent any security breaches or other negative impacts to the Commonwealth.

The business partner's sponsoring agency Information Security Officer (ISO) is responsible for coordinating and leading Commonwealth related cyber incident response when an incident involves the Commonwealth network or the Commonwealth business partner. As part of an incident response, the ISO shall prescribe the necessary incident management steps that may include, but are not

necessarily limited to, disconnecting a system from the network, confiscating hardware for evidence, or providing information for investigative purposes.

Incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources, such as, but not limited to, systems, files, and databases, shall promptly be reported according to the process and timeframes set out in ITP-SEC024 *IT Security Incident Reporting Policy*.

Business Partner Ordering, Billing and Support

Voice and data services for business partners can be ordered by the sponsoring agency through the Commonwealth Telecommunications Services Contract or may be procured by the business partner in coordination with OA/OIT.

An agency may establish billing for all or part of the business partner service. Multiple agencies sponsoring or sharing a single business partner service may share costs based on percentages of use or equally between them. The agency shall negotiate connection costs and billing prior to implementation.

Support is available to Commonwealth business partners under the following conditions:

- The business partner shall provide contact names to the sponsoring agency.

- The sponsoring agency shall provide the authorized business partner contact names to the Commonwealth's TSP.

- The sponsoring agency will provide help desk procedures to the business partner.

- Emergency or outage related help desk support is provided by the Commonwealth's TSP.

- Routine requests for assistance and configuration changes shall be directed to the sponsoring agency.

4.   Responsibilities

4.1   Agencies shall

- Engage ENOS through the Service Request process for all new business partner connections.

- Submit requests for firewall changes, routing changes, or direct business partner-to-business partner connections to OA/OIT on behalf of their sponsored business partners.

4.2   OA/OIT Shall

- Review all business partner service requests.

- Review all requests for business partner firewall and routing changes.

4.3 Third-party vendors, licensors, contractors, or suppliers

- Procure their own internet connection(s).

- Ensure all services provided by the Commonwealth are being used solely for the support of business activities associated with the Commonwealth.

- Access the Commonwealth data network though the designated business partner network.

- Implement appropriate industry standard security solutions, policies, and procedures.

- Promptly report any IT security incidents.

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

- ITP-SEC010 *Virtual Private Network Standards*

- ITP-SEC034 *Enterprise Firewall Rule Set*

- ITP-NET019 *Virtual Desktop Infrastructure*

- ITP-SEC031 *Encryption Standards*

- ITP-SEC024 *IT Security Incident Reporting Policy*

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 are to 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 is to 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	06/18/2004	Base Document	
Revision	12/20/2010	ITP Refresh	
Revision	10/09/2015	• ITP refresh, including updated URLs • Update business partner provisioning • Revised minimum business day turnaround timeframe from three to seven in Telecommunications Services Provided for Business Partners section • Language additions regarding Routing of business partners and clarification that sponsoring agencies are to work with ENS, not business partners. Inclusion of SERP language as the mechanism for conducting new Business Partner connections. • Removed mentions of decommissioned SEC024A	
Revision	06/15/2022	• Updated template and format • Replace definitions with links • Added 3rd parties to the scope • Replaced References to COPPAR with IT Policy Waiver Process • Clarified that business partner- to-business partner communications are not recommended, and use shall be limited to Commonwealth-only business • Updated ENS to ENOS • Guidance was updated for how and when to engage ENOS for business partner connections • Added a section regarding business partner site to site VPN • Clarified business partner security expectations • Added section 4. Responsibilities • Updated references	[Revised IT Policy Redline <06/15/2022>](#)