pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise Firewall Rule Set

ITP Number ITP-SEC034	**Effective Date** August 28, 2008
Category Security	**Supersedes**
Contact RA-ITCentral@pa.gov	**Scheduled Review** May2022

1. Purpose

This Information Technology Policy (ITP) provides a baseline enterprise firewall rule set by identifying the common needs throughout the enterprise regarding Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP) port requirements in order to enable agencies to communicate securely across the enterprise and Internet.

A common firewall policy in any size organization makes responses to external or internal situations more predictable. In addition to providing a level of protection against port scanning, attacks, or software vulnerabilities, a firewall policy provides the organization's local security team with a baseline or starting point in addressing malicious events. If the organization knows the networking requirements of its applications, then the ability to predict the impact of security-related events is enhanced. An event could have many characteristics and take on many different forms. If any of those characteristics involve network port access, a basic rule set offers baseline protection.

2. Scope

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

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.

3. Policy

The baseline firewall rule denies all services. OPD-SEC034A, Enterprise Firewall Rule Set Configurations, identifies those services that are permitted. OPD-SEC034A identifies the most common services used for communications within the Commonwealth's environment. These services are primarily agency-to-enterprise services and enterprise services to agency in nature.

Agencies must perform an audit to identify all "Agency to Agency" and "Agency to Enterprise Service" application protocols to ensure those specific port requirements are documented and then applied to the agencies firewall(s). ITP-SEC031 - *Encryption Standards* defines requirements to encrypt "Agency to Agency" communications.

4. Responsibilities

4.1 Agencies shall comply with the requirements as outlined in this ITP.

4.2 Office of Administration, Office of Information Technology shall comply with the requirements as outlined in this ITP.

4.3 Third-party vendors, licensors, contractors, or suppliers shall comply with the requirements as outlined in this ITP.

5. Related ITPs/Other References

- OPD-SEC034A - *Enterprise Firewall Rule Set Configurations* **(obtain from Agency Information Security Officer)**
- ITP-SEC031 - *Encryption Standards*

6. Authority

- Executive Order 2016-6, 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 Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision	Redline
Original	8/28/2008	Base Policy	
Revision	4/2/2014	ITP Reformat	
Revision	5/10/2021	Policy Refresh Added Exemption Section Third-party vendors added to Scope and Responsibilities Sections	Revised IT Policy Redline <05/10/2021>