pennsylvania
OFFICE OF ADMINISTRATION

# Information Technology Policy
## *Enterprise Firewall Rule Set*

| | |
|---|---|
| **Number**<br>ITP-SEC034 | **Effective Date**<br>August 28, 2008 |
| **Category**<br>Security | **Supersedes**<br>None |
| **Contact**<br>RA-ITCentral@pa.gov | **Scheduled Review**<br>June 2024 |

## 1. Purpose

This Information Technology Policy (ITP) provides the baseline enterprise firewall rule set. This policy identifies 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.

## 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 shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

## 3. Background

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.

## 4. Policy

The baseline firewall rule denies all services. *OPD-SEC034A, Enterprise Firewall Rule Set Configurations*, identifies those services that are permitted and provides information related to the Enterprise GeoIP blocking service. *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 shall 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). Agencies shall refer to *ITP-SEC031, Encryption Standards* for requirements on encrypting "Agency to Agency" communications.

## 5. Responsibilities

### 5.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

### 5.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

### 5.3 Third-party vendors, licensors, contractors, or suppliers shall:

Ensure any devices with access to or hosting Commonwealth data are protected by a perimeter firewall system. An audit shall be performed to identify all application service protocols to ensure specific port requirements are documented and applied to the necessary firewall(s).

## 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*
- *OPD-SEC034A, Enterprise Firewall Rule Set Configurations* (By request only – RA-ITCentral@pa.gov)
- *ITP-SEC003, Enterprise Content Filtering Standard*
- *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*
- *ITP-SEC0010, Virtual Private Network Standards*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC023, Information Technology Security Assessment and Testing Policy*
- *ITP-SEC029, Physical Security Policy for IT Resources*

- *ITP-SEC031, Encryption Standards*
- *ITP-NET018, Commonwealth Metropolitan Area Network (MAN) and Internet Access*
- *ITP-PLT005, Server Operating System Policy*

## 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.

If a determination cannot be made whether a policy waiver is required by the information contained within the tables in *OPD-SEC034A, Enterprise Firewall Rule Set Configurations* - Section 3.4 Network Security Zones; by default, the Agency shall submit a policy waiver for ITP-SEC034 via the enterprise IT policy waiver process.

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 | 8/28/2008 | Base Policy | N/A |
| Revision | 4/2/2014 | ITP Reformat | N/A |
| Revision | 5/10/2021 | • Policy Refresh<br>• Added Exemption Section<br>• Third-party vendors added to Scope and Responsibilities Sections | N/A |
| Revision | 08/09/2021 | Updated Related ITPs Section | N/A |
| Revision | 03/25/2022 | Utilizing Accessible ITP template<br>Enterprise GeoIP blocking language added to policy<br>Policy links added | N/A |
| Revision | 05/27/2022 | Third party requirement within Responsibilities section was updated. | N/A |
| Revision | 11/07/2022 | Added Background section and moved appropriate language to it.<br>Updated Scope to make inclusive of connection to Commonwealth Network.<br>OPD-SEC034A updated. | N/A |

| Version | Date | Purpose of Revision | Redline Link |
|---|---|---|---|
| Revision | 06/13/2023 | Consolidated Reference, Authority, Publication Version Control and Exemption from OPD-SEC034A into this ITP.<br>Scope third party vendor statement and Responsibilities section for third party vendors updated. | Revised IT Policy Redline <06/13/2023> |