



Information Technology Policy

Enterprise Firewall Rule Set

ITP Number ITP-SEC034	Effective Date August 28, 2008
Category Recommended Policy	Supersedes
Contact RA-ITCentral@pa.gov	Scheduled Review Annual

This Information Technology Policy (ITP) establishes policy for the commonwealth's enterprise firewall rule set.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to provide 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 security 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 Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

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 insure those specific port requirements are documented and then applied to the agencies firewall(s). ITP-SEC031 - *Encryption Standards for Data in Transit* defines requirements to encrypt "Agency to Agency" communications.

4. References

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

5. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

6. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

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

Version	Date	Purpose of Revision
Original	8/28/2008	Base Policy
	4/2/2014	ITP Reformat