

Information Technology Policy

Enterprise Policy and Software Standards for Agency Firewalls

ITP Number ITP-SEC011	Effective Date January 31, 2002
Category Security	Supersedes
Contact RA-ITCentral@pa.gov	Scheduled Review May 2022

1. Purpose

This Information Technology Policy (ITP) establishes an enterprise-wide security policy designed to augment privacy, authentication, and security via deployment of network firewalls. In addition, this ITP establishes a firewall software standard. The purpose of this policy is to help ensure the security of Commonwealth information technology (IT) assets, and to allow the Commonwealth to meet and fully comply with federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

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. Objective

The objective of this policy is to establish policy and standards for network firewalls.

4. Policy

This ITP establishes an enterprise-wide policy for agency Municipal Area Network (MAN) gateway firewalls.

- All agencies connected to the Commonwealth MAN are required to implement a firewall at the gateway to their networks.
- Agencies are to adhere to at least the baseline firewall policy rule set as identified in ITP-SEC034 – *Enterprise Firewall Rule Set*.
- Additional rules and permissible accesses may be added to the baseline firewall policy rule set and implemented to provide network accessibility to meet the requirements of the agency.

- The agency's firewall will work in conjunction with the Commonwealth enterprise firewalls, Network Intrusion Prevention Systems (NIPS), Network Intrusion Detection Systems (NIDS), and Host Intrusion Prevention System (HIPS) to provide the necessary security for the agency network.
- Existing non-standard and stand-alone firewalls still may be utilized but if replaced, new firewalls are to comply with the firewall standards defined in this ITP.

The Office of Administration/Office for Information Technology (OA/OIT) will function as the coordination point for all firewalls that agencies wish to establish between the agency's Local Area Networks (LANs) and the Commonwealth MAN (including wide area connections). Agencies are to contact the Security Operations Section prior to purchasing and installing firewalls.

Agencies are to coordinate all firewall implementations with the Enterprise Security Operations section to ensure that appropriate rule sets are in place to maintain the highest level of security and to support interoperability between multiple firewalls. This policy does not preclude any agency from utilizing router filters in conjunction with firewalls to enhance network security.

5. Standards

CURRENT STANDARDS

(These technologies meet the requirements of the current architecture and are recommended for use.)

Technology	Platforms	Category	Technology Classification
Firewall-1 / Provider-1 / (by Checkpoint Technologies, Ltd.)	--	--	Current

CONTAIN

(These technologies no longer meet the requirements of the current architecture and are not recommended for use. They will be phased out over time. No date has been set for their discontinuance.)

Technology	Platforms	Category	Technology Classification
--	--	--	Contain

RETIRE

(These technologies are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology	Platforms	Category	Technology Classification
--	--	--	--

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research technologies are less widely accepted, and time will determine if they will become a standard.)

Technology	Platforms	Category	Technology Classification
N/A	--	--	Emerging / Research

6. Responsibilities

- 6.1 Agencies shall comply with the requirements as outlined in this ITP.
- 6.2 Office of Administration, Office of Information Technology shall comply with the requirements as outlined in this ITP.
- 6.3 Third-party vendors, licensors, contractors, or suppliers shall comply with the requirements as outlined in this ITP.

7. Related ITPs/Other References

- ITP-SEC034 – *Enterprise Firewall Rule Set*

8. Authority

- Executive Order 2016-06, Enterprise Information Technology Governance

9. 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.

10. 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	01/31/2002	Base Policy	
Revision	04/16/2009	Removed references to Layer one and two security protection and rescinded ITB I.6	
Revision	04/2/2014	ITP Reformat; Merge STD-SEC001A into ITP	
Revision	01/28/2021	Updated Bureau name update and removed Data Power House.	
Revision	05/05/2021	Policy Refresh Added Exemption Section Added third-party vendors to scope and responsibilities sections	Revised IT Policy Redline <05/05/2021>