pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise Policy and Software Standards for Agency Firewalls

ITP Number ITP-SEC011	***Effective Date*** January 31, 2002
Category Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

This Information Technology Policy (ITP) establishes enterprise-wide policy and standards for network firewalls.

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 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. 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.

- The Data Power House (DPH) will implement a firewall at the gateway to the DPH network. Agencies that have specific firewall configuration requirements are to relay them to their DPH contact.

- 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 agencies' Local Area Networks (LANs) and the Commonwealth MAN (including wide area connections). Agencies are to contact the OA Bureau of Infrastructure and Operations (OA/BIO) prior to purchasing and installing firewalls.

Agencies are to coordinate all firewall implementations with the Enterprise Network Security Team 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. Related ITPs/Other References

- ITP-SEC034 – *Enterprise Firewall Rule Set*

7. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

8. 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	1/31/2002	Base Policy
Revision	4/16/2009	Removed references to Layer one and two security protection and rescinded ITB I.6
	4/2/2014	ITP Reformat; Merge STD-SEC001A into ITP