pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Anti-Virus Technology Standards

ITP Number ITP-APP034	***Effective Date*** November 20, 2009
Category Recommended Policy	***Supersedes***
Contact RA-itcentral@pa.gov	***Scheduled Review*** April 2015

This Information Technology Policy (ITP) establishes enterprise-wide standards and policies for Anti-Virus technology.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish enterprise-wide standards and policies for Anti-Virus technology.

2. Background

Setting and implementing Anti-Virus technology standards benefits the Commonwealth through increased enterprise security and streamlining patch management.

Anti-Virus software is designed to detect and prevent viruses from infecting machines. Often these viruses are transmitted via e-mail. It proactively stops and removes malicious software, extends coverage against new security risks, and reduces the cost of responding to outbreaks.

Anti-virus software provides the following capabilities:

- Blocks a broad range of viruses and malicious codes
- Scans memory for malicious code
- Limits outbreak damage, even before .DAT files are issued
- Closes ports, monitors applications, and e-mails engines
- Blocks files and directories
- Traces and blocks sources of infection
- Protects e-mail programs
- Optimizes updating for remote systems

- Locks down files
- Detects advanced rootkit

3. 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.

4. Policy

Agencies are to adhere to the standards in section 5 of this ITP.

Agencies are to refer to ITP-SEC001 - *Enterprise Host Security Software Suite Standards and Policy* for virus definition policy and standards.

5. Standards

CURRENT STANDARDS

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

Technology	Products	Technology Classification
Virus Protection Software	McAfee VirusScan 8.7	Current

Notes regarding Current Products:

- All products are to be patched with service packs within six months of the release date in accordance with ITP-SYM006 - *Desktop and Server Software Patching Policy.*
- These are technologies that are supported by the standards and meet the requirements of the architecture.
- They are recommended for use and purchase.
- The review cycle for these technologies is to take place on a semiannual basis and is to be applied on an as-needed basis throughout the cycle.

CONTAIN

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

Technology	Products	Technology Classification

Virus Protection Software	McAfee VirusScan versions prior to 8.7	Contain

Notes Regarding Contained Products:

- Technologies that are no longer the standard. They will be phased out over time.
- Extensive modifications to these systems require review to determine if newer technology is to be used.
- All products are to be patched with service packs within six months of the release date in accordance with *ITB-SYM006.*
- New deployments or installations of these products are not recommended.

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	Products	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	Products	Technology Classification
-	-	-

Notes Regarding Research and Emerging Technologies:

- Technologies that have potential to become current and may be suitable for test environment.
- Require a waiver request to be used in a limited production mode.

6. Related ITPs/Other References

- ITP-PRO001 – *IT Procurement Review Process*
- ITP-SEC001 - *Enterprise Host Security Software Suite Standards and Policy*
- ITP-SYM006 - *Desktop and Server Software Patching Policy*

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	9/18/2008	Base Document
	10/25/2010	Move McAfee VirusScan 8.5 to contained; Current is now 8.7
	4/2/2014	ITP Reformat; Merged STD-APP034A into ITP