pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise Host Security Software Suite Standards and Policy

ITP Number	***Effective Date***
ITP-SEC001	August 28, 2008
Category	***Supersedes***
Recommended Policy	OPD-SEC001A, RFD-SEC001B, OPD-SEC001C
Contact	***Scheduled Review***
RA-ITCental@pa.gov	May 2014

This Information Technology Policy (ITP) establishes standards for use of the commonwealth's antivirus agent, host intrusion prevention agent, incident response servlet and patch management for all servers, workstations, and laptops connecting to the commonwealth network.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish the standards for use of the commonwealth's antivirus agent, host intrusion prevention agent (host-based intrusion prevention system), incident response servlet and patch management agent for all servers, workstations, and laptops connecting to the commonwealth network, and to define related policy for enterprise host intrusion prevention software for servers at the Office of Administration/Office for Information Technology/Bureau of Infrastructure and Operations/Enterprise Server Farm. This includes equipment located in the 'co-location' and 'managed services' areas of the Enterprise Data Center (EDC).

The intention of this policy is to ensure that any systems under the control of the agencies that have the potential for introducing a virus or other malicious program onto the commonwealth network are protected by the referenced security agent software. Benefits to be realized through the establishment and use of standard tools for these security agents include, but are not limited to:

- Enterprise licensing for the specified product suite, thereby ensuring acquisition cost savings for the commonwealth.
- Enterprise-level support for the selected product suite, ensuring centralized availability and consistency of support services.
- Consistency in the execution of security policies and in the identification and analysis of security events.

Several supplemental documents are included with this ITP detailing the standards being established for the security agents described, and providing supporting information on the operational use of these agents within the commonwealth. Some of these documents may not be available to the public.

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. Background

This ITP applies to all microcomputer-class servers, workstations, and laptops connecting to the Commonwealth Enterprise Metropolitan Area Network (MAN) used by any agencies, departments, boards, commissions or councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to participate in the solutions, but may require separate license and support contracts to do so.

4. Objective

The objective of this ITP is to establish standard software tools and describe the Office of Administration/Office for Information Technology (OA/OIT) service offering, which will be used to protect all servers, workstations, laptops, and other TCP/IP-based equipment from computer-borne viruses; malicious software, (such as malware, keystroke logging software, etc.); or exploits of software vulnerabilities throughout the commonwealth.

5. Policy

The OA/OIT requires all agencies to use all of the prescribed standard tools (see section 7 of this ITP for the current standards) for each of the following endpoint security tools in their detection/removal or blocking/prevention modes at all times. In order for these tools to be most effective, all agencies must follow the operating system and application patching standards established in ITP-SYM006.

Anti-Virus Protection: This solution is the Commonwealth's standard mechanism to update virus signature files and scan engines; distribute updated enterprise policies to detect, clean, and/or remove computer viruses and other malicious code using the Commonwealth's standard enterprise anti-virus software; and monitor compliance with Commonwealth anti-virus standards.

Host Intrusion Prevention: This solution is the Commonwealth's standard host intrusion prevention system to detect and prevent unauthorized application and/or network behavior on desktops, servers, laptops and tablet devices and to distribute updated enterprise policies.

Incident/Forensic Response Encase Servlet: This solution is the Commonwealth's standard for performing incident response on desktops, servers, laptops and tablet devices. This solution is also used to perform virus and other malicious program investigations and remediation.

Agencies are required to utilize the most current approved versions of these enterprise standard software products real-time scanning, detection and removal, and blocking capabilities at all times. This applies to all desktops, servers, laptops and tablet devices to in order to protect these devices against infection or compromise of the Commonwealth computer network by blocking, detecting and removing malicious code.

Agencies are required to follow the minimum detection, prevention, removal, and blocking standard policies set at the enterprise level to prevent such exploits at all times with the real-time scanning features of these endpoint security products.

All servers are required to utilize the Host Intrusion Prevention Systems (HIPS) portion of the enterprise endpoint protection standard solution at all times in blocking mode on desktops, servers, laptops and tablet devices for High Priority (sometimes referred to as Critical/Emergency priority detections) in order to protect against malicious Internet attacks.

The OA/OIT utilizes enterprise-level control and monitoring of these security solutions in order to protect critical technology assets. All agencies are required to participate in the enterprise deployment, management and monitoring of the aforementioned security solutions.

Failure to follow the Enterprise policies and standards may result in the blockage of non-compliant devices from accessing the Commonwealth network. Failure to keep devices up–to-date may result in those devices being denied access to the Commonwealth network. OA/OIT, through authority granted by the Enterprise Security Initiatives Memorandum of Understanding, may use enterprise-level authority to update agency devices, after appropriate escalation and notification procedures have been followed, if non-compliance is seen as an urgent threat to the security of the Commonwealth network.

6. Responsibilities

The following tables provide an overview of the roles and responsibilities related to the operation and management of the host security. Further detail on operational procedures can be obtained by contacting the appropriate Office of Administration/Office for Information Technology (OA/OIT) bureau or department.

Note: Agency in the following table means all departments, boards, commissions and councils under the Governor's jurisdiction as defined within this ITB, as well as other entities connecting to the Commonwealth Network.

Anti-Virus Agent Roles and Responsibility	Agency	OA/OIT/BIO
Provide, manage and operate centralized anti-virus management software application and servers.		X
Maintain and enforce agent policies to enforce minimum commonwealth standards for anti-virus protection on all servers, workstations, laptops wireless and related devices utilized within the commonwealth.		X
Provide enterprise support in the configuration/maintenance and use of the standard anti-virus products for Agencies under the Governor's jurisdiction. Contact Information: OA/OIT Enterprise Security Team at (717) 772-8606		X
Use the commonwealth's standard software for anti-virus for all desktops, file and print servers; or, convert to the standard anti-virus product (if they are not currently using the standard).	X	

Install & maintain appropriate anti-virus monitoring and management agent on all servers, workstations, laptops, wireless and related devices utilized within the commonwealth.	X	X
Ensure the standard software's scan engine and DAT files are up to date on all desktops, file and print servers, database/application servers, Internet servers, etc. accessing the commonwealth computer network. All agency implementations are to meet the minimum Enterprise Base ePO configuration requirements as published on the Commonwealth Portal. Agencies may create additional more stringent policy rules at their discretion. The responsibility to actively monitor these devices and keep them up to date with current anti-virus scan engines and signature files also applies to non-commonwealth computer users.	X	
OA/OIT will publish the changes to the Enterprise AV & HIPS policies for a two week timeframe for agency testing and comment. (OA/OIT or an Agency can request a waiver from the two week timeframe to accelerate the testing/implementation phase, to refine the proposed change in scanning/protection policy, or to request exemption from the scanning/protection policy standard.)	X	X
Actively monitor desktops to ensure compliance with Anti-Virus standards.	X	X
Agencies are to promptly investigate incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and data bases. Agencies are to evaluate cyber security incidents according to the "IT Incident Reporting Procedures and Form" provided in SEC024. The completed form is to be submitted via e-mail to Pennsylvania-Computer Security Incident Response Team (PA-CSIRT) or online to the PA-CSIRT Web Portal, within the timeframes stated in SEC024. The IT Security Incident Reporting Form is to be filled out within the timeframes stated in SEC024.	X	
Run periodic reports identifying devices that are not compliant with the commonwealth standard anti-virus software.		X
Review the periodic non-compliance reports provided by OA/OIT and update every device listed on the report. Run weekly compliance reports from the centralized, enterprise anti-virus management and reporting console and update every device listed on the report.	X	
Provide agencies with the capability to access dedicated enterprise support technicians from the commonwealth's standard anti-virus software vendor to assist with technical issues.		X

Provide toll free telephone support to non-dedicated support technicians from the commonwealth standard anti-virus software vendor to assist with technical issues without direct intervention by OA/OIT/BIO staff.		X
Agencies are to provide the commonwealth's Chief Information Security Officer (CISO) with a primary and secondary point of contact for cyber security incident reporting and handling. The agency Information Security Officer (ISO) is to be the primary point of contact. Agencies are to provide names, work phone numbers, mobile phone numbers, home phone numbers, and work and home e-mail addresses for those points of contact. Agencies are to notify the CISO as soon as possible, when changes occur to the contact list. Agencies will be given permissions to track, update, and provide remediation information for security incidents online through the PA-CSIRT Web Portal.		X
Ensure that any copies of the Commonwealth of Pennsylvania's anti-virus software or compliance monitoring software agents owned by the commonwealth that are installed on non-commonwealth computer user devices are removed upon the termination of the entity providing services to the Commonwealth of Pennsylvania and the Agency.	X	
Monitor and remain abreast of issues related to the McAfee software and any emerging virus threats and issue appropriate security alerts to designated agency representatives.		X

Enterprise Host Intrusion Prevention Agent Roles and Responsibility	**Agency**	**OA/OIT/BIO**
Provide, maintain and monitor a centralized host intrusion prevention solution for the commonwealth. Includes management of the vendor relationship.		X
Maintain and enforce an enterprise level agent policy to enforce minimum commonwealth standards for host intrusion prevention protection on all servers, workstations and laptops utilized within the commonwealth.		X
Provide enterprise support in the configuration/maintenance and use of the standard host increasing prevention products for Agencies under the Governor's jurisdiction. Contact Information: OA/OIT Enterprise Security Team at (717) 772-8606		X
Install and maintain the standard host intrusion prevention systems agent on all servers, desktops and laptops and ensure agents are communicating with the enterprise central site.	X	
Adhere to enterprise policies and settings established for the host intrusion prevention agents.	X	
Provide enterprise level compliance and incident reporting as stated in policies SEC024.		X

Actively monitor systems for intrusions and other security related incidents and respond accordingly to security events.	X	X
Follow mandatory incident reporting policies and procedures as stated in policies SEC024.	X	

Enterprise Encase Servlet Installation Roles and Responsibility	**Agency**	**OA/OIT/OIS**
Provide, maintain and monitor a centralized host Enterprise Encase Safe Server for an Incident response solution for the commonwealth. Includes management of the vendor relationship.		X
Maintain and enforce an enterprise level servlet agent deployment to enforce minimum commonwealth standards for incident response on all servers, workstations and laptops utilized within the commonwealth.		X
Provide enterprise support in the deployment/ configuration/maintenance and use of the standard, Encase Enterprise product for agencies under the Governor's jurisdiction.		X
Initial installation of the EnCase Servlet agent on all servers, desktops and laptops and ensure agents are communicating with the Enterprise EnCase Safe.	X	X
Maintenance and installation of updates to the EnCase Servlet agent on all servers, desktops and laptops and ensure agents are communicating with the Enterprise Encase Safe.	X	X
Provide enterprise level compliance and auditing with policies SEC024.		X
Follow mandatory incident reporting policies and procedures as stated in policies SEC024.	X	
Ensure agency and/ or host based firewalls have active connectivity to enable the encase servlets to communicate back to the Central Server.	X	X
Ensure appropriate network information and subnets are included on the Enterprise Safe and kept current.	X	X
Actively monitor systems for Encase servlet agent installation, intrusions and other security related incidents and respond accordingly to security events.	X	X

Systems Management Agent Roles and Responsibility	**Agency**	**OA/OIT/BIO**
Provide, manage, and operate a centralized patch management compliance reporting and distribution solution.		X
Provide functional specification, required configuration, and operational documentation to support enterprise patch management solutions, standards, and procedures.		X
Design, implement and operate all current and future patch management solutions, standards and procedures as described in the OA/OIT supplied functional specification, required configuration and operational documentation.	X	X

Support the installation and maintenance of functional patch management server(s) and client software on all Commonwealth of Pennsylvania assets running approved desktop, laptop, mobile device and server operating system software.	X	X
Connect all Commonwealth of Pennsylvania computing assets to patch management server every 30 days (minimum) to report patch compliance status.	X	
Provide level 1 support services to agencies using the OA/OIT managed site through the Enterprise Help Desk.		X
Provide two contacts (primary and secondary) for patch management related initiatives and communications.	X	

7. Standards

7.1 CURRENT STANDARDS

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

Product	Platforms	Technology Classification
Anti-Virus McAfee VirusScan Enterprise 8.7i (Patch 5 or higher) McAfee VirusScan Enterprise Anti-Spyware 8.7i McAfee VirusScan Enterprise 8.8i (Patch 2 or higher) McAfee VirusScan Enterprise Anti-Spyware 8.8i McAfee VirusScan Enterprise for Macintosh 9.x McAfee VirusScan Enterprise for Linux 1.7 or higher McAfee Event Policy Orchestrator (ePO) 4.6 McAfee Agent 4.0 (Windows 2000 OS Only) McAfee Agent 4.6 SiteAdvisor Enterprise 3.5.x	All desktops and servers, laptops, wireless and related devices covered by the enterprise license agreement. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 2003, Windows 2008, Windows 2012, Linux (Red Hat, SUSE, Ubuntu & CentOS), HP-UX, AIX, Sun Solaris desktops, servers, and laptops that have been issued licenses by Office of Administration/Office for Information Technology.	Current
McAfee Host Intrusion Prevention for Desktop 8.0 (Patch2 or higher) McAfee Host Intrusion Prevention for Server 8.0 (Patch 2 or higher)	Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 2003, Windows 2008, Windows 2008, Windows 2012, Linux (Red Hat, SUSE, Ubuntu	Current

Product	Platforms	Technology Classification
	& CentOS), HP-UX, AIX, Sun Solaris desktops, servers, and laptops that have been issued licenses by Office of Administration/Office for Information Technology.	
Incident Response Encase Servlet	All Windows desktops and servers, laptops, wireless and related devices that have been issued licenses by the commonwealth.	Current
Patch Management Microsoft System Center Configuration Manager (SCCM)	All Windows desktops and servers, laptops, wireless and related devices that have been issued licenses by the commonwealth.	Current

7.2 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.

Product	Platforms	Technology Classification
McAfee Agent 4.0 (All Operating Systems but Windows 2000 devices being retired) McAfee LinuxShield 1.6.x McAfee VirusScan Enterprise for Linux 1.6.x SiteAdvisor Enterprise 3.0 (Patch 0 or higher)	All desktop and servers, laptops, wireless and related devices	Contain
Host Intrusion Prevention Software	Windows (all versions), Linux, Unix	Contain
Patch Management Microsoft Software Update Services (SUS) Microsoft Window Server Update Services (WSUS)	All desktop and servers, laptops, wireless and related devices	Contain
Patch Management Microsoft Systems Management Server 2003 (SMS 2003)	All Windows desktops and servers, laptops, wireless, and related devices that have been issued licenses by the commonwealth.	Contain

7.3 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.

Product	Platforms	Technology Classification
McAfee Agent 3.x McAfee Agent 4.0 and 4.5 McAfee Event Policy Orchestrator (ePO) 4.0 & 4.5	All Operating Systems	Retire 6/30/2013
Host Intrusion Prevention Software Host Intrusion Prevention Software McAfee Host Intrusion Prevention for Desktop 7.0 (all versions) McAfee Host Intrusion Prevention for Server 7.0 (all versions) McAfee Host Intrusion Prevention 6.0 Host Intrusion Prevention Agent ISS Desktop Host Intrusion Prevention Agent ISS RealSecure Server	Windows (all versions) desktops, servers, and laptops that have been issued licenses by Office of Administration/Office for Information Technology.	Retire 9/30/2013 9/30/2009 9/30/2009 9/30/2009
Anti-Virus McAfee VirusScan 4.51 SP 1 McAfee VirusScan Enterprise 7.1 Symantec NAV McAfee VirusScan Enterprise 8.0i McAfee VirusScan Enterprise 8.5i McAfee VirusScan Enterprise Anti-Spyware 8.5i McAfee MacTel 8.0 & 8.5 (Macintosh Intel processors) McAfee MacTel 8.6.1 (Macintosh Intel processors) McAfee Virex 7.7 (Macintosh G-series processors) McAfee LinuxShield 1.2 SP 1 & SP 2, 1.3, 1.4, 1.5, 1.5.1 McAfee LinuxShield 1.5.1 McAfee Event Policy	All desktop and servers, laptops, wireless and related devices	 Retire 6/30/2008 Retire 6/30/2008 Retire 6/30/2008 Retire 6/30/2009 Retire 6/30/2009 Retire 6/30/2008 Retire 6/30/2008 Retire 6/30/2013 Retire 6/30/2013 Retire 6/30/2013 Retire 6/30/2013

Orchestrator (ePO) 4.0 McAfee Event Policy Orchestrator (ePO) 3.6.0 McAfee Event Policy Orchestrator (ePO) 3.5		Retire 6/30/2010 Retire 6/30/2009 Retire 6/30/2008
Host Intrusion Prevention Agent ISS RealSecure Server ISS RealSecure Desktop Protector ISS Legacy Products (BlackICE) Others	Windows (all versions), Linux, Unix	Retire 12/31/2006
Patch Management Microsoft Systems Management Server (SMS) 2.0 Shavlik Products (e.g., HFNetChk, NetChk) Novell ZENworks Others	All desktop and servers, laptops, wireless and related devices	Retire 06/30/2006

7.4 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.

Product	Platforms	Technology Classification
Anti-Virus McAfee MOVE 2.x & 3.x for Virtual Desktops McAfee MOVE 2.x & 3.x for Virtual Servers Policy Auditor 6.x Risk Advisor 2.x McAfee AV for Mobile Devices	All desktop and servers, laptops, wireless, and related devices	Emerging
Host Intrusion Prevention Agent	Windows	Emerging
Host Intrusion Prevention Agent	Linux, Unix	Emerging
Patch Management Vintella (Quest) VMX	Linux, Unix	Research

8. Enterprise Endpoint Security Suite License Agreements Coverage

Currently, the Office of Administration/Office for Information Technology (OA/OIT) maintains enterprise-level software license agreements for the following Desktop and Server Security Software:

- McAfee Total Virus Defense Suite (includes: VirusScan Enterprise for Windows, VirusScan for Linux, VirusScan for Macintosh, AV for Mobile devices, ePO, and other anti-virus software tools)
- Microsoft Systems Management Server 2003 (SMS 2003)
- System Center Configuration Manager (SCCM)

Each licensing agreement has unique requirements which are detailed below.

Provisions for McAfee Anti-Virus Agreement
Agencies, departments, boards, commissions, and councils under the Governor's jurisdiction are now licensed with McAfee to use the McAfee anti-virus software. Each agency may copy the software as many times as necessary to protect all of its computing devices.

Commonwealth employees utilizing VPN connections into the commonwealth network from these agencies may copy software for home use on non-commonwealth-owned PCs, connecting to the commonwealth network through VPN, to diminish the likelihood of contaminating desktops when transferring files/diskettes and e-mail between home and the workplace.
Contractors and other non-commonwealth entities may use the anti-virus software on workstations and laptops used to provide services to the commonwealth during the tenure of their commonwealth contract at no additional expense.

The contract includes anti-virus products for the following platforms and Web applications:
- Desktops using Windows 2000, XP, Vista, 7, 8, 2003, 2008, 2012, Millennium
- Wintel and Netware servers using Windows NT, 2000, XP, Vista, 7, 8, 2003, 2008, 2012
- Wireless Devices
- Windows CE Devices
- Macintosh PCs
- Linux/Unix-based Workstations and Servers
- Microsoft Exchange Servers
- Virtual Servers & Desktops running on the VMWare, Microsoft & Citrix Virtual Platforms
- Mobile Devices utilizing the Android OS

Provisions for SMS 2003
Initial server and client license purchases were made for agencies that did not have the resources to purchase their own. Moving forward, it is the responsibility of each agency to budget for, procure, and maintain the appropriate number of SMS and related licenses as necessary to remain compliant with this policy.

Provisions for System Center Configuration Manager (SCCM)
All agencies that upgrade to System Center Configuration Manager 2007 will be required to connect to the commonwealth central site and follow the SCCM Standards Documentation and Procedures that will be maintained by the Enterprise SMS/SCCM team on a secure website available only to the commonwealth.

9. Related ITPs/Other References

- ITP-SEC024 - *Information Technology Security Incident Reporting Policy*
- Minimum Enterprise Base ePO Configuration

10. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

11. 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	8/26/2008	Base Document
	10/16/2008	Updated to include System Center Configuration Manger (SCCM).
	10/16/2008	Product Standards updated to include System Center Configuration Manger (SCCM).
	6/22/2009	Replaced IBM /ISS Proventia Agent with McAfee HIPS agent
	4/1/2010	Product Standards updated to reflect current versions of McAfee security products
	1/6/2012	Product Standards updated to reflect current versions of McAfee security products
	8/21/2013	Product Standards updated to reflect current versions of McAfee security products; systems management/patching moved to ITB-SYM006. Changed TCP/IP-based equipment to network-based equipment
	4/2/2014	ITP Reformat; Merged OPD-SEC001A, RFD-SEC001B, OPD-SEC001C into ITP