pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise Host Security Software Suite Standards and Policy

ITP Number ITP-SEC001	**Effective Date** August 28, 2008
Category Security	**Supersedes** OPD-SEC001A, RFD-SEC001B, OPD-SEC001C
Contact RA-ITCental@pa.gov	**Scheduled Review** March 2018

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 (OA/OIT/BIO) 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.

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 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.

4. Policy

OA/OIT requires all agencies to use all of the prescribed standard tools (refer to RFD-SEC001A - *Enterprise Host Security Anti-Virus Software 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 *Commonwealth IT Resources Patching Policy*.

5. Definitions

- **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.
- **Advanced Persistent Threat Endpoint Protection:** This solution is the Commonwealth's host-based malware protection program from FireEye called "HX" that integrates with the FireEye network based devices for network (NX), email (EX) and fileshare (FX) for the detection, containment and mitigation of advanced malware.

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 ITP, 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 ePO Team at OA/OIT Virus Support.		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 and 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. 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 anti-virus and host intrusion protection systems 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 ITP-SEC024 *IT Security Incident Reporting Policy*. The completed form is to be submitted via e-mail to Pennsylvania-Computer Security Incident Response Team at RA-CISO@pa.gov or online to the PA-CSIRT Incident Reporting tool, within the timeframes stated in ITP-SEC024. The IT Security Incident Report is to be completed within the timeframes stated in ITP-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 at ra-CISO@pa.gov 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 Incident Reporting tool.		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 anti-virus 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 intrusion prevention products for agencies under the Governor's jurisdiction. Contact Information: OA/OIT ePO Team at OA/OIT Virus Support.		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 ITP-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 ITP-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 Enterprise EnCase 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 ITP-SEC024.		X
Follow mandatory incident reporting policies and procedures as stated in policies ITP-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 EnCase 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 thirty (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	

FireEye HX Endpoint Agent Roles and Responsibility	Agency	OA/OIT/EISO
Provide, manage, and operate a centralized advanced persistent threat (APT) endpoint 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 FireEye HX 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 FireEye HX 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 FireEye HX management console every day (minimum) to report status.	X	
Provide level 1 support services to agencies using the EISO managed solution.		X
Provide two contacts (primary and secondary) for FireEye HX management related initiatives and communications.	X	

7. Standards

(Refer to RFD-SEC001A - *Enterprise Host Security Anti-Virus Software Standards* for anti-virus software standards.)

Product	Platforms	Technology Classification
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

8. Related ITPs/Other References

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- RFD-SEC001A - *Enterprise Host Security Anti-Virus Software Standards*
- Enterprise Access Protection Policy – Protection/Endpoint - https://itcentral.pa.gov/Security/Pages/Services.aspx (Limited Access)
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC024 - *Information Technology Security Incident Reporting Policy*
- ITP-SYM006 – *Commonwealth IT Resources Patching Policy*

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. Publication Version Control

It is the 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.

11. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

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

Version	Date	Purpose of Revision
Original	08/26/2008	Base Document
Revision	10/16/2008	Updated to include System Center Configuration Manger (SCCM)
Revision	10/16/2008	Product Standards updated to include System Center Configuration Manger (SCCM).
Revision	06/22/2009	Replaced IBM /ISS Proventia Agent with McAfee HIPS agent
Revision	04/01/2010	Product Standards updated to reflect current versions of McAfee security products
Revision	01/06/2012	Product Standards updated to reflect current versions of McAfee security products
Revision	08/21/2013	Product Standards updated to reflect current versions of McAfee security products; systems management/patching moved to ITP-SYM006. Changed TCP/IP-based equipment to network-based equipment
Revision	04/02/2014	ITP Reformat; Merged OPD-SEC001A, RFD-SEC001B, OPD-SEC001C into ITP
Revision	03/09/2016	Removed Background section Added definition to Definitions section Added language for FireEye HX endpoint software for APT Removed Contain and Retire Standards Migrated Current A/V standards to RFD-SEC001A Removed Section 8 "License Agreement Coverage" Removed outdated language throughout
Revision	03/22/2017	Added reference to Enterprise Protection document Revised a number of URLs Updated contact information