pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Enterprise Host Security Software Policy

ITP Number	Effective Date
ITP-SEC001	August 28, 2008
Category	**Supersedes**
Security	OPD-SEC001A, RFD-SEC001B, OPD-SEC001C
Contact	**Scheduled Review**
RA-ITCental@pa.gov	February 2022

1. Purpose

This Information Technology Policy (ITP) establishes the standards for use of the Commonwealth's Endpoint Security, incident response servlet, and patch management agent used for IT Resources connecting to the Commonwealth network.

The intention of this policy is to ensure that any systems under the control of the agencies that have the potential for introducing malware 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 ITP applies to all departments, offices, 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.

3. Definitions

3.1 Advanced Persistent Threat Endpoint Protection: A capability that allows for detection and containment of advanced malware.

3.2 Anti-Virus Protection: A capability to detect and quarantine both known and unknown malware through static signatures, heuristic signatures, and machine learning.

3.3 Endpoint Detection and Response (EDR): A capability that provides:

- Real time indication on known tactics, techniques, and procedures (TTPs);
- The ability to monitor common applications and processes for exploitations and proactively block those exploitations; and
- The ability to detect and block lateral movement within the enterprise network

3.4 Endpoint Security: an integrated solution that provides cybersecurity protection on endpoint devices including servers, desktops, laptops, and other mobile devices and should encompass the below capabilities, have the ability to integrate with different security solutions utilized by the Commonwealth, automatically update signature files and scan engines.

3.5 Host Intrusion Prevention System (HIPS): A capability to detect and prevent unauthorized application and/or network behavior on desktops, servers, laptops and tablet devices and to distribute updated enterprise policies.

3.6 Forensic Response Servlet: A capability for performing forensic captures on desktops, servers, laptops and tablet devices which enables OA/OIT forensic team to investigate security incidents.

3 Policy

The Office of Administration, Office for Information Technology (OA/OIT) requires the use all the prescribed standard tools, detailed in RFD-SEC001A *Enterprise Host Security Anti-Virus Software Standards*, to be in detection/removal or blocking/prevention modes at all times. 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*.

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

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

All endpoints are required to utilize the HIPS portion of the enterprise endpoint protection solution when unsupported by the EDR solution.

OA/OIT utilizes enterprise-level controls 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 Information Technology Policies and standards may result in the blockage of non-compliant devices from accessing the Commonwealth network. OA/OIT 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.

4 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 OA/OIT.

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

EDR Roles and Responsibility	Agency	OA/OIT
Provide, manage, and operate centralized EDR management software application and servers.		X

Maintain and enforce agent policies that require 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 EDR 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 EDR for all desktops, servers; or, convert to the standard anti-virus product (if they are not currently using the standard).	X	
Install and maintain appropriate EDR 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, and servers,. 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 Enterprise will publish the changes to the enterprise EDR 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 Incident Response Procedures document provided in ITP-SEC024 *IT Security Incident Reporting Policy*.	X	
Run periodic reports identifying devices that are not compliant with the Commonwealth standard EDR 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 EDR 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 EDR software vendor to assist with technical issues.		X
Provide toll free telephone support to non-dedicated support technicians from the Commonwealth standard EDR software vendor to assist with technical issues without direct intervention by OA/OIT/ETSO 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	X
Ensure that any copies of the Commonwealth's EDR 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 and the agency.	X	X
Monitor and remain abreast of issues related to the EDR 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**
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	X
Adhere to enterprise policies and settings established for the host intrusion prevention agents.	X	X
Provide enterprise level compliance and incident reporting as stated in policies ITP-SEC024 *IT Security Incident Reporting Policy*.		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	

Installation Roles and Responsibilities	**Agency**	**OA/OIT**
Provide, maintain, and monitor a centralized host 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 security solutions for agencies under the Governor's jurisdiction.		X

Initial installation of the Forensic Response Servlet agent on all servers, desktops and laptops and ensure agents are communicating with Forensic Response central server.	X	X
Maintenance and installation of updates to the agent on all servers, desktops and laptops and ensure agents are communicating with the enterprise solution.	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 *IT Security Incident Reporting Policy*.	X	
Ensure agency and/ or host-based firewalls have active connectivity to enable the servlets to communicate back to the Forensic Response central server.	X	X
Ensure appropriate network information and subnets are included on the enterprise solution and kept current.	X	X
Actively monitor systems for agent installation, intrusions and other security related incidents and respond accordingly to security events.	X	X

Systems Management Agent Roles and Responsibilities	**Agency**	**OA/OIT**
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 computing assets to patch management server, at a minimum, every thirty (30) days 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	

Endpoint Agent Roles and Responsibilities	**Agency**	**OA/OIT**
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 Endpoint Agent 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 Endpoint Agent management server(s) and client software on all Commonwealth assets running approved desktop, laptop, mobile device, and server operating system software.	X	X
When online, connect all Commonwealth computing assets to an Endpoint Agent management console, at least once a day to report status.	X	
Provide level 1 support services to agencies using the EISO managed solution.		X
Provide two contacts (primary and secondary) for Endpoint Agent management related initiatives and communications.	X	

5 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

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- RFD-SEC001A *Enterprise Host Security Standards* (*Authorized CWOPA personnel access only. Contact RA-ITCentral@pa.gov for requests*)
- Enterprise Access Protection Policy – Protection/Endpoint - https://itcentral.pa.gov/Security/Pages/Services.aspx (*Limited Access*)
- ITP-ACC001 *Information Technology Digital Accessibility Policy*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC024 *Information Technology Security Incident Reporting Policy*
- ITP-SYM006 – *Commonwealth IT Resources Patching Policy*

6 Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

7 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.

8 Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, 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. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	08/26/2008	Base Document	N/A

Revision	10/16/2008	Updated to include System Center Configuration Manger (SCCM)	N/A
Revision	10/16/2008	Product Standards updated to include System Center Configuration Manger (SCCM).	N/A
Revision	06/22/2009	Product Standards updated to reflect current versions	N/A
Revision	04/01/2010	Product Standards updated to reflect current versions	N/A
Revision	01/06/2012	Product Standards updated to reflect current versions	N/A
Revision	08/21/2013	Product Standards updated to reflect current versions systems management/patching moved to ITP-SYM006. Changed TCP/IP-based equipment to network-based equipment.	N/A
Revision	04/02/2014	ITP Reformat; Merged OPD-SEC001A, RFD-SEC001B, OPD-SEC001C into ITP.	N/A
Revision	03/09/2016	Removed Background section Added definition to Definitions section Added language 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	N/A
Revision	03/22/2017	Added reference to Enterprise Protection document Revised a number of URLs Updated contact information	N/A
Revision	06/14/2019	Classified RFD-SEC001a as Confidential Removed references to products throughout	Revised IT Policy Redline <06/14/2019>
Revision	2/09/2021	Revised definitions Clarified language throughout Removed “ETSO” from Responsibilities tables Revised RFD-SEC001A	Revised IT Policy Redline <2/09/2021>