Information Technology Policy

Enterprise Host Security Software Policy

Number ITP-SEC001	**Effective Date** August 28, 2008
Category Security	**Supersedes** All prior versions
Contact RA-ITCentral@pa.gov	**Scheduled Review** June 2023

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 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 offices, departments, 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.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Definitions

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

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

4.3 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 exploitation and proactively block those exploitations; and
- The ability to detect and block lateral movement with the enterprise network.

4.4 Endpoint Security: An integrated solution that provides cybersecurity protection on endpoint devices including servers, desktops, laptops, and other mobile devices that should encompass the below capabilities:

- The ability to integrate with different security solutions utilized by the Commonwealth; and
- Automatically update signature files and scan engines.

4.5 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 distribute updated enterprise policies.

4.6 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.

4. Policy

The Office of Administration, Office for Information Technology (OA/OIT) requires the use of all the prescribed standard tools, detailed in STD-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-SEC041 *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.

4.1 Host Security Roles and 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. 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 shall promptly investigate incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to IT resources such as systems, files, and data bases. Agencies shall evaluate cyber security incidents according to the Incident Response Process document provided in ITP-SEC024 *Cyber Security Incident Response and 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 shall 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) shall be the primary point of contact. Agencies shall provide names, work phone numbers, mobile phone numbers, home phone numbers, and work and home e-mail addresses for those points of contact. Agencies shall 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

5. Responsibilities

5.1 Agencies shall comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office of Information Technology shall comply with the requirements as outlined in this ITP.

5.3 Third-party vendors, licensors, contractors, or suppliers shall:

- Provide a mandatory information security awareness training and education program to all their employees and contractors.
- Ensure compliance with federal and state guidelines and regulations regarding the collection, maintenance, use, and security of IT Resources, as defined in Management Directive 205.34.
- Ensure implementation of prudent, reasonable, and effective practices for the protection and security of IT Resources, which includes the protection of Class "C" Classified Records or Closed Records, as defined in ITP-SEC019, against accidental or deliberate unauthorized disclosure, modification, or destruction
- Implement procedures for responding to incidents, breaches, or misuse of IT Resources, as outlined in ITP-SEC024.

- Implement processes for protecting Class "C" Classified Records or Closed Records during transmission, processing, and storage.
- Implement procedures to mitigate overall and specific risks of breach or misuse of Commonwealth IT Resources and the damages and costs associated with a breach or misuse. This would include patching, internal and external scanning, and monitoring.
- Utilize industry standard antivirus, anti-malware, Host Intrusion Prevention, incident response procedures, monitoring, reporting, network, and application firewalls in accordance with ITP-SEC001 for real-time scanning, detection, removal, and blocking of potentially malicious content.

6. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx
- 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 Amended 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 *Cyber Security Incident Response & Reporting Policy*
- ITP-SEC041 *Commonwealth IT Resources Patching Policy*
- STD-SEC001A *Enterprise Host Security Anti-Virus Software Standards*

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. 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 shall be directed to RA-ITCentral@pa.gov.

9. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Policy 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	N/A
Revision	2/09/2021	Revised definitions Clarified language throughout Removed "ETSO" from Responsibilities tables Revised RFD-SEC001A	N/A
Revision	06/09/2022	ITP Refresh References to SYM006 updated to SEC041 References to OPD-SEC001A updated to STD-SEC001A Added policy links. Updated link to Archer GRC tool. Added third party language to Scope and Responsibilities.	Revised IT Policy Redline <06/09/2022>