Information Technology Policy

Enterprise Host Security Software Policy

Number	**Effective Date**
ITP-SEC001	August 28, 2008
Category	**Supersedes**
Security	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	July 2024

1. Purpose

This Information Technology Policy (ITP) establishes the policy, responsibilities, and procedures for the utilization of the Commonwealth's endpoint security, incident response servlet, and patch management agent for IT Resources connecting to the Commonwealth network.

The intention of this policy is to ensure that IT Resources under the control of agencies that have the potential for introducing malware into the Commonwealth network are protected by the standardized security agent software. Benefits to be realized through the establishment and utilization of standardized tools for these security agents include, but are not limited to:

- Enterprise licensing for the specified product suite(s), thereby ensuring acquisition cost savings for the Commonwealth.
- Enterprise-level support for the selected product suite(s), ensuring centralized availability and consistency of support services across all agencies.
- 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 and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

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

3. Policy

The Office of Administration, Office for Information Technology (OA/IT) requires the use of all the prescribed standard tools, detailed in *STD-SEC001A, Enterprise Host Security Software Standards* (*Authorized CWOPA user access only)*.

To ensure adequate and consistent protection of Commonwealth IT resources, these tools shall be in detection/removal or blocking/prevention modes at all times. In order to ensure their effectiveness, all agencies shall follow the IT Resources patching standards established in *ITP-SEC041, Commonwealth IT Resources Patching Policy*.

Agencies shall utilize the most current, approved versions of these enterprise standard software products at all times for real-time scanning, detection/removal, and blocking/prevention capabilities. This applies to all IT Resources in order to protect these devices against infection or compromise of the Commonwealth network by blocking, detecting, and removing malware.

All endpoints are required to utilize the Host Intrusion Prevention System (HIPS) portion of the enterprise endpoint protection solution when unsupported by the Endpoint Detection and Response (EDR) solution.

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

Failure to follow IT Policies and standards may result in the blockage of non-compliant devices from accessing the Commonwealth network. OA/IT 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.

3.1 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/IT Virus Support.

EDR Roles and Responsibility	Agency	OA/IT
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, desktops, and laptops utilized within the Commonwealth.		X
Provide enterprise support in the configuration, maintenance and use of the standard EDR products for agencies.		X
Use the Commonwealth's standard software for EDR for all servers, desktops, and laptops, 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, desktops, and laptops, utilized within the Commonwealth.	X	X

Ensure the standard software's scan engine and DAT files are up to date on all servers, desktops, and laptops 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 Service Organizations.	X	
OA/IT 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/IT 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 servers, desktops, and laptops to ensure compliance with anti-virus standards.	X	X
Promptly investigate incident involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to IT Resources such as systems, files, and databases.	X	
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/IT 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/IT/ Enterprise Technology Services Office (ETSO) staff.		X
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 and mobile phone numbers, and work e-mail addresses for those points of contact. The CISO shall be notified as soon as possible at ra-CISO@pa.gov when changes occur within agency point of contacts.	X	
Provide Agencies necessary permissions to track, update, and provide remediation information for security incidents online through the PA-CSIRT Incident Reporting tool for their primary and secondary points of contact.		X
Ensure that any Commonwealth-owned and installed copies of EDR software or compliance monitoring software agents on Service Organization 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

4. Responsibilities

4.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

4.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

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

- Promptly investigate any suspected security incidents. Implement procedures for responding to and reporting incidents, breaches, or misuse of IT Resources, as outlined in ITP-SEC024.
- Utilize the Commonwealth's standard software or an industry standard for EDR on all servers, desktops, and laptops that are utilized to access or host Commonwealth data.
- Ensure systems which access or host Commonwealth data are being actively monitored and run weekly reports to ensure compliance with EDR and anti-virus standards.
- 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 (ITP-SEC041 *Commonwealth IT Resources Patching Policy*), internal and external scanning (ITP-SEC023 *IT Security Assessment & Testing Policy*), 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.
- Ensure the names, work and mobile phone numbers, and work email addresses for a primary and backup contact are provided to the Commonwealth CISO at ra-ciso@pa.gov.

5. 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
- *STD-SEC001A, Enterprise Host Security Software Standards* (*Authorized CWOPA User Access only. Any other requests, contact RA-ITCentral@pa.gov.*)
- 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-SEC019, Policy & Procedures for Protecting Commonwealth Electronic Data*

- *ITP-SEC024, Cyber Security Incident Response & Reporting Policy*
- *ITP-SEC035, Mobile Device Security Policy*
- *ITP-SEC041, 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 shall 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 ITP, a request for a policy waiver shall 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 RFD-SEC001A updated to STD-SEC001A Added policy links. Updated link to Archer GRC tool. Added third party language to Scope and Responsibilities.	N/A
Revision	07/18/2023	Added clarity to policy language and ensured consistency among overall policy language (intent not changed). Replaced definitions with links to the glossary. Scope updated to include any entity connecting to COPA network. Third-party vendor responsibilities were updated consistent with requirements in ITP.	Revised IT Policy Redline <07/18/2023>