Enterprise Host Security Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
June 30, 2026

Supersedes:
ITP-SEC001, ITP-SEC032

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) establishes the policy for connecting to the Commonwealth network and establishes the enterprise standards and controls that must be met to deploy Data Loss Prevention (DLP) technologies or solutions.

3. Scope

This policy 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 policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

4.1 Host Security

The Office of Administration, Office for Information Technology (OA/IT) requires the use of all the prescribed standard tools, detailed in the *Enterprise Host Security Standard*.

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 the *Patch Management Policy*.

Agencies shall always utilize the most current, approved versions of these enterprise standard software products for real-time scanning, detection/removal, and

blocking/prevention capabilities. This applies to all IT Resources 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 blocking of non-compliant devices from accessing the Commonwealth network. OA/IT may, after appropriate escalation and notification procedures have been followed, use enterprise-level authority to update agency devices, if non-compliance is seen as an urgent threat to the security of the Commonwealth network.

4.1.1 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. Agencies shall complete any needed testing and provide any comment within two weeks of publication. (OA/IT or an agency can request a waiver from	X	X

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).		
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 the *IT Security Incident Reporting Policy.* Service Organizations are responsible for reporting cyber security incidents to the applicable agency as soon as reasonably practical upon discovery of a cyber security incident. Agencies are to be notified no later than the time period specified in the applicable terms of the contract and in accordance with the Pennsylvania Data Breach Notification Act.	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 current on issues related to the EDR software and any emerging virus threats and issue appropriate security alerts to designated agency representatives.		X

DLP technologies may exist in several forms including host-based (server or endpoint) or network-based solutions. DLP services help the organization comply with standards and regulations. It helps protect sensitive information and prevents unintended disclosure.

DLP technologies do not negate the need for users to utilize caution and adhere to all applicable policies (such as, but not limited to the *Data Classification Policy* and regulations to protect PII and sensitive data from accidental compromise and misuse.

4.2 Technical Requirements for DLP Solutions

Any DLP technology/solution must comply with the technical specifications and requirements outlined in the following CommonwealthITP's:

- *eCommerce Policy*
- *Data Classification Policy*
- *Encryption Policy*

Note: This ITP establishes the enterprise baseline minimum requirement for DLP. Agencies may set additional policy requirements to meet their specific compliance criteria due to additional laws, statues, or regulations such as CJIS Security Policy, IRS Pub 1075, PCI, HIPAA, etc.

4.3 Reporting Incidents of Data Compromise

The Agency ISO or designee shall conduct investigations into incidents involving potential or confirmed compromises of Commonwealth Data. Any confirmed or suspected compromises shall be reported in accordance with the *IT Security Incident Reporting Policy*.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the

revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document