pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy
Enterprise Web Application Firewall

Number ITP-SEC004	**Effective Date** January 15, 2010
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** January 2025

1. Purpose

This Information Technology Policy (ITP) establishes the policy and enterprise-wide standards for Web Application Firewalls.

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

In order to ensure the highest levels of security and overall effectiveness of protecting Internet-facing web applications, compliance rule sets will be invoked by the Enterprise Information Security Office (EISO) to automatically block attacks coming from the Internet.

Internet-facing web applications, regardless of where they are hosted, shall adhere to the Web Application Firewall (WAF) standards for protecting Commonwealth electronic data.

All internet-facing web applications which contain Sensitive Security, Protected, or Privileged Information, as defined by *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*, are required to utilize a WAF as directed in *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*.

All Internet-facing web applications which contain Prerequisite-Required Information or Public Records, as defined in *ITP-INF015*, are recommended to utilize a WAF as directed in *ITP-SEC019*. Agencies shall refer to *STD-SEC004A, Web Application Firewall Product Standards* (*Authorized COPA user access only*) for a current listing of WAF standards.

All existing Internet-facing web applications containing Sensitive Security, Protected, or Privileged Information, as defined in *ITP-INF015*, not currently secured by a WAF shall adhere to this guidance prior to the next scheduled annual review (12 months) of this ITP. Any applications not in compliance after 12 months will require an approved IT Policy Waiver and Risk Assessment and Acknowledgement document (*OPD-SEC040A, Risk Assessment and Acknowledgement*).

3.1 Web Application Security Controls

Other WAF security control standards include, but are not limited to, the following:

- All WAF traffic shall be HTTPS.
- A business-determined mission critical Internet-facing web application infrastructure that can be secured by either a hardware or software form factor.
- The WAF may not disallow an authorized request from an Internet user and may not affect legitimate business traffic in the IT infrastructure while protecting web applications.
- The WAF default configuration must be able to monitor and prevent specific web application attacks until emergency patches and/or source-code changes can be made to the vulnerable web application.
- The default web application rule configuration must be able to monitor and immediately block types of Web attacks targeting the web application.
- An SSL certificate is required by the WAF to inspect data passed between the web servers.
- The WAF must be able to track, log, and inspect the following information relating to the web applications access by the end-user:
  - Application layer network traffic;
  - External and internal user sessions;
  - External and internal user-encrypted sessions;
  - Simulated attacks;
  - Blocked attacks; and
  - HTTP, HTTPS, Proxy error logging to Security Information and Event Management (SIEM).
- Real-time automated failover architecture is required when the WAF is integrated inline and could impact the flow of business-critical network traffic.

3.2 Monitoring

In accordance with *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, communication with a Commonwealth authorized user may be audited by the EISO on a random basis to ensure compliance with set WAF protection rules.

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 Commonwealth Chief Information Security Officer (CISO) shall:

Regularly audit for compliance with this policy and its associated standards.

4.4 Agency Information Security Officers (ISOs) or designees shall:

Ensure Agency Internet-facing web applications are protected in accordance with this ITP.

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

Implement a WAF to protect all Commonwealth data regardless of data classification-level. In addition, the WAF shall:

- Minimize the threat window for each exposure by blocking access to the vulnerability until the vulnerability can be fixed in the source code;
- Meet PCI, HIPAA, CJIS Security Policy, IRS Publication 1075, and Privacy compliance requirements where appropriate to the supporting agency;
- Monitor end-user transactions with a web application; and
- Provide an additional layer of web application hardening Open Web Application Security Project (OWASP) protection.

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-SEC004a, Web Application Firewall Product Standards* (Authorized COPA user access only)
- *ITP-SEC034,* Enterprise Firewall Rule Set
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*

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	01/15/2010	Base Document	N/A
Revision	04/2/2014	ITP Reformat; Merged OPD-SEC004B, STD- SEC004A into ITP	N/A
Revision	05/05/2021	Added Definition section. Add Telecom Service provider. Add Cloud Service provider. Add GeoIP blocking. Add IP Reputation Added Exemption from This Policy Section Added third party vendors to Scope and Responsibilities section	N/A
Revision	07/14/2022	ITP Refresh Created STD-SEC004a Moved product standards to STD-SEC004a Added references to STD-SEC004a in Policy and References Minor general policy language updates (no intent changed) Policy references/links updated. Third party vendor requirements added consistent with OPD-SEC000B	
Revision	11/29/2023	Annual Review Scope of internet facing web applications updated in alignment with ITP-SEC019. Required for Sensitive Security, Protected and Privileged Information. Recommended for Prerequisite-required and Public Records. Scope updated based upon a connection to the COPA network and requirements for third parties re-directed to Responsibilities section. Definition moved to OA Glossary, added links to defined word. Objective removed (repetitive language). Reference to sensitive, protected, privileged or prerequisite required information updated to Class "C" or Closed Records with referenced to ITP-INF015. Added link to STD-SEC004A for ease of access. Additional references to ITP-INF015 in Responsibilities and Related ITPs/Other References. Added reference to ITP-SEC034 under Related ITPs/Other References. Renumbered sections. Section 3.1 now WAF Security Controls and 3.2 Monitoring. Updated Responsibilities for Agency ISOs.	N/A

Version	Date	Purpose of Revision	Redline Link
Revision	01/16/2024	Updated policy to only allow HTTPS traffic on WAF.	Revised IT Policy Redline <01/16/2024>