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
July 2023

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 (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 that are applicable to the products and services provided to the Commonwealth.

3. Definitions

3.1 Web Application Firewall (WAF): Addresses the needs of limiting internet attacks and monitoring of web applications located in the Commonwealth. A web application firewall provides a number of key benefits, such as:

- Protecting against web attacks.
- Minimizing the threat window for each exposure by blocking access to a vulnerability until the vulnerability can be fixed in the source code.
- Meeting compliance requirements.
- Monitoring end-user transactions with a web application.
- Providing an additional layer of web application hardening.

4. Objective

To establish policy and enterprise-wide standards for use of the web application firewalls.

5. 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, are encouraged to use the web application firewall standard for protecting sensitive, protected, privileged, or prerequisite required information as directed in ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*. Agencies shall refer to STD-SEC004A *Web Application Firewall Product Standards* for a current listing of WAF standards.

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

- A business-determined mission critical internet-facing web application infrastructure can be secured by either a hardware or software form factor.
- The web application firewall 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 web application firewall 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.
- A SSL certificate is required by the web application firewall to inspect data passed between the web servers.
- The web application firewall 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 web application firewall is integrated inline and could impact the flow of business-critical network traffic.

5.1 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 web application firewall protection rules.

6. Responsibilities

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

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

7.3 Commonwealth Chief Information Security Officer (CISO) shall regularly audit for compliance with this policy and its associated standards.

7.4 Agency Information Security Officers (ISOs) or designees shall ensure Agency internet traffic is in accordance with this ITP.

7.5 Third-party vendors, licensors, contractors, or suppliers shall implement a WAF. The WAF shall be used to protect data classified under ITP-SEC019 as Class "C" Classified Records or Closed Records following the standards set forth in this ITP. 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, and Privacy compliance requirements;
- Monitor end-user transactions with a web application; and
- Provide an additional layer of web application hardening Open Web Application Security Project (OWASP) protection.

7. 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-SEC004a – Web Application Firewall Product Standards
- ITP-SEC019 – Policy and Procedures for Protecting Commonwealth Electronic Data

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. 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.

10. 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	Revised IT Policy Redline <07/14/2022>