pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise Web Application Firewall

ITP Number ITP-SEC004	**Effective Date** January 15, 2010
Category Security	**Supersedes**
Contact RA-ITCentral@pa.gov	**Scheduled Review** May 2022

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. Objective

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

4. Definitions

Web application firewall (WAF): address 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 to the Commonwealth's Enterprise Data Center (EDC) and the agencies that house web applications there. These benefits include:

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

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 to automatically block attacks coming from the Internet. Internet-facing web application located in Commonwealth datacenters are encouraged to use the web

application firewall standard for protecting sensitive, protected, privileged, or prerequisite required information.

Other WAF security control standards include but 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.

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 Enterprise Information Security Office on a random basis to ensure compliance with set Web application firewall protection rules.

6. Product Standards for Web Application Firewalls

CURRENT STANDARDS

(These technologies or products meet the requirements of the current architecture and are recommended for use.)

Technology or Product	Product or Platforms	Technology Classification
Telecom Service Provider	Service Provider Product	Current
Cloud Service Provider	Service Provider Product	Current
iMPERVA (SecureSpere)	Hardware based (Appliance)	Current

CONTAIN

(These technologies or products no longer meet the requirements of the current architecture and are not recommended for use. These technologies are to be phased out over time. No date has been set for their discontinuance.)

Technology or Product	Product or Platforms	Technology Classification
--	--	Contain

RETIRE

(These technologies or products are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology or Product	Product or Platforms	Technology Classification
--	--	Retire mm/dd/yy

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research technologies are less widely accepted and time will determine if they will become a standard.)

Technology or Product	Product or Platforms	Technology Classification
--	--	Emerging / Research

7. Web Application Firewall Compliance Standards

These minimum compliance standards are intended to provide a default set of Web application firewall protection rules to protect Commonwealth data from internet web attacks. The minimum Web application compliance standard consists of protection categories with the following settings:

Web Application Firewall Standard Protection

(A shaded category indicates blocking is enabled for the protection rule)

Category type for a protection rule	Counter measures
Application Buffer Overflow	Sending too much data in a request to the application.
Cross-site scripting (XSS)	Inserting scripting language into text fields to be displayed to other users.

Cookie Poisoning	Modifying the cookie file causing the return of unauthorized information or enabling performance of activity on behalf of another user.
Forceful Browsing	Gaining access to the constrained areas in a Web server directory.
Hidden Field Manipulation	Modifying form fields allowing damaging data to pass to the Web application.
Parameter Tampering	Modify the parameters being passed as part of the URL.
Stealth Commanding (e.g., SQL/OS Injections)	A code injection technique that exploits a security vulnerability occurring in the database layer of an application.
URL & Unicode encoding	Encoding certain characters in the URL to bypass application filters, thus accessing restricted resources on the Web server.
GEOIP Blocking	GEO IP policies are configured to block traffic based on the originating county source.
IP Reputation	A technique for accurate, early, and frequently updated identification of compromised and malicious clients so attackers can be blocked before they target web application.

No additional “protection rules” may appear before these enterprise “protection rules” without approval from the Enterprise Information Security Office.

Agencies may request additional “protection rules” for their agencies’ business requirements by contacting the Enterprise Information Security Office.

8. Responsibilities

8.1 The Commonwealth's Chief Information Security Officer (CISO) will regularly audit for

compliance with this policy and its associated standards.

8.2 Agency Information Security Officers (ISOs) or designates are to ensure agency internet traffic is in accordance with this policy.

8.3 Third-party vendors, licensors, contractors, or suppliers utilizing web application firewalls shall comply with the requirements as outlined in this ITP.

9. 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

- MD 205.34 Amended – *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*

10. Authority

- Executive Order 2016-06, Enterprise Information Technology Governance

11. 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 are to be directed to RA-ITCentral@pa.gov.

12. 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 Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision	Redline Link
Original	01/15/2010	Base Document	
Revision	04/2/2014	ITP Reformat; Merged OPD-SEC004B, STD- SEC004A into ITP	
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	Revised IT Policy Redline <05/05/2021>