Information Technology Policy

Internet Accessible Reverse-Proxy Servers and Services

Number ITP-SEC002	**Effective Date** November 8, 2005
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2023

1. Purpose

This Information Technology Policy (ITP) provides direction regarding the use of Reverse-Proxy Servers and services by Commonwealth agencies and establishes the policy for the utilization of the Office of Administration, Office for Information Technology (OA/OIT) Reverse Proxy Managed Services and the approval process to continue to use existing or obtain new servers and/or services.

The Commonwealth of Pennsylvania has been rapidly deploying mission critical web accessible applications to meet the business needs of the Commonwealth agencies and constituents. Security vulnerabilities and cyber terrorism threats have become common, so it is imperative that the Commonwealth take the necessary steps to ensure the integrity and availability of mission critical applications that rely on Reverse-Proxy Servers by mitigating these vulnerabilities.

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.

3. Definitions

3.1 Reverse-Proxy Server: A type of proxy server that typically sits behind the firewall and directs client requests to the appropriate backend server.

3.2 Reverse Proxy Managed Services: The service follows a defined standardized process to implement reverse proxy requests that includes a Service Request, Solution proposal, and monitoring.

4. Policy

To ensure maximum security within the Commonwealth, OA/OIT maintains Reverse Proxy Managed Services for agency use. Agencies are required to utilize the OA/OIT

Reverse Proxy Managed Services to fulfill their business requirements for Reverse-Proxy Servers and services.

An approved exception waiver is required if an agency desires to implement their own Reverse-Proxy Server and/or utilize the standard reverse proxy service for a web server at an agency location. Due to the criticality of enterprise-wide security standards for web applications, OA/OIT strongly discourages agencies from seeking exemptions to this policy.

Reverse-Proxy Servers, and all corresponding web servers, whether at an OA/OIT enterprise data center location or at an agency location, will be subject to security and vulnerability scans prior to network connectivity and on a regular basis, and will be required to comply with ITP-SEC001 *Enterprise Host Security Software Policy*.

The Enterprise Information Security Office (EISO) will contact the OA/OIT enterprise data center or the respective agency contact, if a security vulnerability exists and/or a security incident occurs on a Reverse-Proxy Server or web server. A timeframe will be established for the required resolution of the concern. If the concern is not addressed within the requested timeframe, OA/OIT will take appropriate action to mitigate the threat.

5. Responsibilities

5.1 Agencies shall comply with the requirements as outlined in this ITP. Any agency seeking an exemption to this ITP shall refer to Section 9, Exemptions from this Policy for requirements and additional information specific to waivers for this ITP.

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

6. 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
- ITP-ACC001 *Digital Accessibility Policy*
- ITP-SEC001 *Enterprise Host Security Software Policy*

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. 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.

9. 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.

An agency requesting a policy waiver shall include the following in the request:

- Reason why the standard Reverse Proxy Managed Services offering option cannot be used.
- Details about the application, connectivity, server requirements, and equipment location.
- Network diagrams to illustrate the security components that will protect the Reverse-Proxy Server(s) and the corresponding web servers that are housed at the agency or in a co-location space.

OA/OIT will review each waiver request. After the Reverse-Proxy Server waiver has been reviewed, one of the following responses will be forwarded to the agency:

- **Approved** – Web server may reside at agency location(s) and/or Agency managed Reverse-Proxy Server solution may be utilized.
- **Approved with conditions** – Web server can reside at agency location(s); however, it shall utilize the enterprise reverse-proxy services.
- **Disapproved** – Web server shall reside in an OA/OIT enterprise data center.

If an agency is granted an exemption in whole or in part, the agency must install server agents as per ITP-SEC001 *Enterprise Host Security Software Policy* on the Reverse-Proxy Servers and the internal web servers that are serviced by the Reverse-Proxy Server. Additionally, the agency must ensure access through all agency access firewalls to allow EISO to complete required internet and vulnerability scans of these servers.

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	11/8/2005	Base Document	N/A
Revision	4/2/2014	ITP Reformat	N/A
Revision	06/04/2021	Updated Bureau Names Changed policy name from proxies to reverse proxies Added Definitions Section Added Third party vendors to Scope and Responsibilities Sections	N/A
Revision	07/12/22	Updates to Purpose Removed third party vendor language from policy Moved details on waiver/exemptions from Responsibilities Section to Exemption Section. Added note in Responsibilities to account for details being moved to Exemption Section. Updated References section and links in policy.	Revised IT Policy Redline <07/12/2022>