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
November 2024

1. Purpose

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

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").

3. Background

The Commonwealth of Pennsylvania has been deploying mission critical web accessible applications to meet the business needs of 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.

4. Definitions

Commonwealth Datacenter Location: A datacenter managed by the Commonwealth or a service organization on behalf of the Commonwealth. This includes separate physical datacenters and the Commonwealth managed cloud environments.

5. Policy

To ensure maximum security within the Commonwealth, OA/IT maintains Reverse Proxy Managed Services for agency use. Agencies are required to utilize the OA/IT Reverse Proxy Managed Services to fulfill their business requirements for Reverse-Proxy Servers and Services.

An approved IT policy waiver is required if an agency has a technical limitation that requires the implementation of its own Reverse-Proxy Server and/or utilization of a 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/IT strongly discourages agencies from seeking exemptions to this policy.

Reverse-Proxy Servers, and all corresponding web servers, whether at a Commonwealth Datacenter Location or at an agency location, will be subject to security and vulnerability scans prior to network connectivity and on a regular basis thereafter, and will be required to comply with *ITP-SEC001, Enterprise Host Security Software Policy*. Agencies shall refer to *ITP-SEC005, Commonwealth Application Certification and Accreditation* and *ITP-SEC023, Technical Security Assessments Policy* for further policy guidance regarding the requirements for security and vulnerability scans.

The Enterprise Information Security Office (EISO) will create and assign a security incident ticket in Archer (governance, risk and compliance tool) to the SOA/IT Enterprise Data Center (EDC) Information Security Officer (ISO) or the respective agency ISO 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 remediation based on the severity level of the security incident ticket and in alignment with *ITP-SEC024, IT Security Incident Reporting Policy*. If the concern is not addressed within the requested timeframe, OA/IT will take appropriate action to mitigate the threat.

6. Responsibilities

6.1 Agencies shall:

Comply with the requirements as outlined in this ITP. Any agency seeking an exemption to this ITP shall refer to Section 10, Exemptions from this Policy for requirements and additional information specific to waivers for this ITP.

6.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

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*
- *ITP-ACC001, Digital Accessibility Policy*

- *ITP-SEC001, Enterprise Host Security Software Policy*
- *ITP-SEC005, Commonwealth Application Certification and Accreditation*
- *ITP-SEC023, Technical Security Assessments Policy*
- *ITP-SEC024, IT Security Incident Reporting Policy*

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.

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

- Reason(s) why the standard Reverse Proxy Managed Services offering option cannot be used.
- Details about the application, data classification(s), 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/IT will review each waiver request and 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 a Commonwealth Datacenter Location.

Regardless of the response received, the agency shall ensure server agents as per *ITP-SEC001, Enterprise Host Security Software Policy* are installed on the Reverse-Proxy Servers and the internal web servers that are serviced by the Reverse-Proxy Server. Assets managed by the Enterprise in a Commonwealth Datacenter Location will have the required agents per *ITP-SEC001* installed as part of the service offering. Additionally, the agency shall ensure access through all agency access firewalls to allow EISO to complete required security 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	11/08/05	Base Document	N/A
Revision	04/02/14	ITP Reformat	N/A
Revision	06/04/21	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.	N/A
Revision	11/29/23	Annual Review General verbiage clean up with no change in intent throughout policy. Scope updated based on connection to Commonwealth Network. Additional text from Purpose moved under new Background section. Section 4 Definitions, previous definitions moved to OA Glossary and linked within policy. New term and definition added for Commonwealth Datacenter Location. Updated references to an OA/IT enterprise data center location to a Commonwealth Datacenter location. Section 5 Policy, updated language from an agency desire/want to a technical limitation as a requirement to submit a waiver. References added within policy language to ITP-SEC005 and ITP-SEC023 for requirements related to security and vulnerability scans. Notification to agency aligned with current process of Archer ticket assignment and remediation in alignment with ITP-SEC024. Section 10, language added to note that Commonwealth Datacenter locations will have agents installed per ITP-SEC001 as part of service offering.	Revised IT Policy Redline <11/29/2023>