Information Technology Policy

Web Server/Application Server Standards

Number ITP-PLT019	**Effective Date** October 26, 2005
Category Platform	**Supersedes** All Prior Versions
Contact RA-ITCentral@pa.gov	**Scheduled Review** January 2024

1. Purpose

This Information Technology Policy (ITP) establishes enterprise-wide standards and guidance for web information and web application servers. Establishing web application server standards will provide guidance to agencies as they plan for new application development projects or make significant investments in existing applications.

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 as outlined in the Responsibilities Section.

The scope of this policy is currently limited to Commonwealth on-premises implementations. Externally hosted solutions (including Commonwealth managed cloud computing environments) are not addressed by the policy at this time.

3. Background

The need for this ITP has evolved out of some basic patterns that have emerged in enterprise architecture. One of these patterns is the three-tier model for enterprise computing. Associated with the three-tier model is the implementation of a Services Oriented Architecture (SOA), since a SOA utilizes elements of all three tiers. Application severs reside the middle tier in the three-tier model and as a host for Web services in a services-oriented architecture.

Application Servers have three basic functions – communicating with back-end systems like business applications or databases, communicating with front-end clients usually Web clients, and providing a framework to execute business logic.

Application servers are widely categorized into three main types, the web information server (web server/HTTP server), the component broker, and the web application server. A web information server utilizes HTML templates and scripts to generate pages. These pages incorporate data from the databases they are connected to. Additionally, web information servers host web services.

A component broker server provides database access and transaction processing services to software components. This includes dynamic link libraries (DLLs), common object request broker architecture (CORBA), and enterprise JavaBeans. Their function can be broken down to two stages. The first stage involves providing the environment for server-side components. The second stage involves providing access to the database and other services.

A web application server supports and provides the rich environment for server-side logic expressed as objects, rules, and components. They are best suited for business logic, eCommerce, and decision processing. Web application servers are designed specifically to extend web information servers to support dynamic content. The web application server software "hooks in" to the web information server software and automatically intercepts any user requests for dynamic content. The web information server still sends out static web pages and graphic files. However, the application server can create dynamic content by mixing data with templates, running programs, components, and services, or by accessing databases.

All the three types of servers mentioned are stateless servers, which unlike the stateful servers; need database or transaction monitors for completing transactions.

4. Definitions

Component Management: The manager that handles all the components and the run time services such as session management, synchronous/asynchronous client notifications, and executing business logic.

Fault Tolerance: The ability of the server with no single point of failure to define policies for recovery and fail-over recovery in the case of the failure of one or more object or group of objects.

Load balancing: The server’s ability to send the request to the different servers within the set-up, depending on the load and availability of the servers.

Mission Critical Application: Any application which, if interrupted for a predetermined period of time, would cause hardship to a segment of the people of the Commonwealth, adversely affect public health and safety, seriously inhibit the primary function of an agency and/or state government operations, or cause any legal liability on behalf of the Commonwealth.

Transaction Management: The transactional capabilities of the server.

5. Policy

Web information and application servers for Mission Critical Applications shall incorporate Fault Tolerance and Load Balancing. Non-Mission Critical Applications use is recommended as a best practice.

Agencies shall adhere to the guidance provided in *ITP-SEC004, Enterprise Web Application Firewall* and *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data* to properly secure web applications and the data they handle. Additionally, all web applications are subject to the Commonwealth Application Certification and Accreditation (CA)[2] process as outlined in *ITP-SEC005, Commonwealth Application Certification and Accreditation*.

All new application development projects shall use one of the current standard Web Application and Information Servers as defined in *STD-PLT019*.

All IT Investments related to application development shall be reviewed prior to inception for compliance with this standard through *ITP-BUS002, IT Investment Review Process*. Major revisions to existing applications that are not using the current standards will be reviewed as part of the IT Investment Review Process to determine if the investment warrants a change in standards at that time.

6. Responsibilities

6.1 Agencies shall:

Ensure that any new web or application servers comply with the requirements of this policy and the standards defined in *STD-PLT019, Web Server/Application Server Standards.*

6.2 Office of Administration, Office for Information Technology shall:

Review all new IT projects and any major revisions to existing applications as part of the *ITP-BUS002, IT Investment Review Process* to determine compliance with this policy.

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

Comply with the requirements as outlined in this ITP that are applicable to the products or services they are providing to the Commonwealth. If the products or services being provided by the third-party vendor, licensor, contractor, or supplier do not fall within the scope of this ITP, compliance is implied. If the third-party vendor, licensor, contractor, or supplier subsequently deploys products or services that fall within the scope of this ITP in the future, compliance with the policy is required.

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-BUS002, IT Investment Review Process*
- *ITP-SEC000, Information Security Policy*
- *ITP-SFT000, Software Development Life Cycle (SDLC) Policy*
- *ITP-SFT002, Commonwealth of PA Design Standards*
- *ITP-SEC004, Enterprise Web Application Firewall*
- *ITP-SEC005, Commonwealth Application Certification and Accreditation*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC041, Commonwealth IT Resources Patching 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.

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	10/25/2005	Base Document	N/A
Revision	12/18/2008	Added paragraph to policy section concerning applications not using current standards	N/A
Revision	04/17/2009	Updated content and references only	N/A
Revision	10/25/2010	ITB Refresh	N/A
Revision	04/02/2014	ITP Reformat; Merged STD-APP002A, STD-APP002B to ITP	N/A
Revision	07/01/2017	• Migration from APP ITP domain to PLT ITP domain • Removed Retire Status tables • Remove Objectives section • Moved Background section language into Policy • Removed Background section	N/A
Revision	01/30/2023	• Added clarification in purpose section that the policy does not currently address externally hosted solutions (guidance and standards are being developed).	Revised IT Policy Redline <01/30/2023>

		• Added third parties to the scope of the policy. • Added background section and moved some content there • Updated definitions • Added requirement that web information and application servers for Mission Critical Applications incorporate Fault Tolerance and Load Balancing • Moved standards to new supplemental policy document STD-PLT019A • Added and updated references throughout	