
Information Technology Policy

Open Source Software

| | |
|---|---|
| <i>ITP Number</i> ITP-APP020 | <i>Effective Date</i> November 24, 2008 |
| <i>Category</i> Recommended Policy | <i>Supersedes</i> |
| <i>Contact</i> RA-itcentral@pa.gov | <i>Scheduled Review</i> April 2015 |

This Information Technology Policy (ITP) establishes enterprise-wide policy for Open Source Software.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to implement policy regarding the use of Open Source Software (OSS) by Commonwealth agencies. OSS is software for which the source code has been made available (according to license terms) for review, modification, deployment, and redistribution.

2. Background

The potential benefits of using open source software are ease of acquisition, faster time to production, transparency, and freedom from vendor lock-in, enhanced ability and greater control for internal support and, often, cost savings. The potential risks include license compliance issues, inefficient maintenance and support, security issues, and poor integration or interoperability, all of which can lead to failure to realize cost savings. Adhering to the guidelines in this ITB will assist in mitigating these risks so the benefits can be realized.

Addressing Potential Risks:

- **Legal issues.** Each license is to be reviewed along with the intended purpose of the OSS product. This review can be accomplished internally at each agency and will be necessary for large and mission critical systems. Obtaining legal counsel is necessary to assess the impact of the license provisions. Regardless of the size or importance of the system, the OA/Legal Information Technology Contracting Office (ITCO) is available to assist agency's legal offices in reviewing license agreements as necessary.

- **Support and Maintenance.** Because the source code is freely available, organizations are not limited to obtaining support from the authors. Mature open source projects have large communities which provide online support, tutorials, and published reference material. When support, service, or infrastructure solution requirements for open source software exceed what an organization is prepared or trained to provide, suppliers or third parties are sometimes available to fill the gap. The availability of required support is to be evaluated early in the project planning phase and the additional cost factored into the total cost of ownership.
- **Security Issues.** Security issues surrounding the use of open source software are similar to the issues surrounding proprietary software in that vulnerabilities may be discovered after the implementation. Whereas proprietary software vendors often adhere to a maintenance schedule for release of fixes, OSS projects often release fixes as issues are identified and corrected. This presents a different maintenance model that an agency is to take into consideration when evaluating whether to use OSS.
- **Integration.** Integration and interoperability issues need to be addressed when evaluating an OSS solution or a proprietary solution. Integration between commercial/proprietary software and OSS is facilitated by increasing vendor involvement with and the move toward the adoption of open industry standards. Due diligence is required when analyzing a new component to fit into an existing information technology infrastructure.

The maturity of an OSS project and its community affects the required skills and resources to support it. Different gaps in maturity require different skill sets. For example, a beginner may be able to overcome a lack of thorough documentation, but fixing bugs in the software may be more difficult. A beginner will expect all the features to be included in the OSS project, whereas an advanced or expert level team can add the features as needed. If the OSS project has a small community, more time may be required to read source code, experiment, and develop an understanding of the OSS product.

It is important to consider the configuration and infrastructure requirements of an OSS solution. Understanding, managing, and maintaining the source code, components, services and software pre-requisites and post-requisites are essential to successful implementation. In some cases, open source solutions use other open source solutions to implement functionality. As an example, some OSS may be maintained in a community repository that requires a source control client to retrieve the open source content. Another example is an open source solution that is designed to use an open source repository.

What OSS Does Not Include

OSS is not to be confused with freeware, which is not officially supported and the functionality of which cannot be validated because source is not available. Refer to ITP-APP033 - *Use of Freeware Policy*, for more information and guidance on freeware. OSS also is not to be confused with shareware, which is trial-version software that can be used free for a limited period of time.

3. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor’s jurisdiction. Agencies not under the Governor’s jurisdiction are strongly encouraged to follow this ITP.

4. Objectives

The objective of this policy is to:

- Provide a policy that identifies the procedure to obtain approval for the use of OSS.
- Establish agency responsibility regarding the implementation of OSS.

5. Policy

Agencies considering the use of OSS are to ensure the technology solution is selected based on best value after careful consideration of all possible alternatives.

Agencies are to use software adopted as a current product standard in any of the existing Office of Administration/Office for Information Technology (OA/OIT) ITPs.

Agencies desiring to obtain and/or deploy OSS that is not named in an ITP are to submit a procurement review/waiver request and obtain approval from the Technical Architecture Review Board. Refer to ITP-PRO001 – IT Procurement Review Process and ITP-BUS004 – IT Waiver Review Process, for detailed information.

Agencies desiring to install OSS to either a desktop or server platform are to coordinate with their respective support organizations for the management of those platforms.

Agencies are responsible for support and inventory control of OSS. Agencies planning to use OSS in production are to test and validate the OSS in a development environment to ensure security and quality control.

Agencies are to adhere to Commonwealth standards for applying security related patches to OSS products. See ITP-SYM006 - *Desktop and Server Software Patching Policy*, for detailed information.

Agencies are to consult with their legal office regarding the rights and responsibilities conferred by the particular OSS license associated with the solution.

Agencies are responsible to ensure that adequate legal review has been performed prior to distributing any source code. This ensures the proper license agreement has been obtained, any distribution conditions have been met, and that indemnification risks associated with use and distribution have been addressed.

6. Related ITPs/Other References

- ITP-PRO001 – *IT Procurement Review Process*
- ITP-APP033 - *Use of Freeware Policy*
- ITP-BUS004 – *IT Waiver Review Process*

7. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

8. Publication Version Control

It is the user’s responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

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

| Version | Date | Purpose of Revision |
|----------|------------|--|
| Original | 11/24/2008 | Base Document |
| | 10/25/2010 | ITB Refresh |
| | 4/2/2014 | ITP Reformat |
| | 7/14/2014 | Included ITP-BUS004 as a reference ITP |