pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Software Licensing

ITP Number ITP-SFT001	**Effective Date** February 22, 2017
Category Software	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** February 2018

1. Purpose

The purpose of this Information Technology Policy (ITP) is to implement policy regarding the use of freeware, Open Source Software (OSS), and Software as a Service (SaaS) by commonwealth agencies.

2. 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.

3. Background

A common misconception is that freeware, shareware, and OSS can be used without restriction. However, these software options are usually covered by licensing and usage requirements. Agencies must understand and adhere to the requirements that may apply to these software options and implement procedures to monitor their installation, usage, copying, and disposal in accordance to those requirements.

It is important for agencies to understand the various benefits and risks associated with the different acquisition and usage models that apply to each of these software options. Benefits are usually classified under two main categories: faster implementation and reduced costs. Risks typically include license/agreement compliance issues, security exposures, lack of maintenance/support/transition procedures, and performance/availability issues. Agencies must define and implement mitigation plans to ensure the anticipated savings are realized.

4. Definitions

4.1 Freeware

Software that is unsupported, available free of charge and can be used for unlimited time in a manner consistent with its end-user agreement.

4.2 Open Source Software (OSS)

Software for which the source code has been made available (according to license terms) for review, modification, deployment, and redistribution.

4.3 Shareware

Software that is licensed for free (possibly with restricted use or functionality) for a limited period of time, but payment is expected for full usage or functionality.

4.4 Software as a Service (SaaS)

Software that is not licensed but available only on a hosted platform, i.e. "the cloud", and can be used in accordance to the service agreement.

4.5 Trial-Version Software

Software that is not considered freeware as defined by this policy and may be used for limited testing in production environments without going through a waiver process.

5. Objective

To establish policy governing the selection and usage of these software options and to effectively communicate agency responsibilities.

6. Policy

6.1 Freeware

6.1.1 Usage

Freeware offers potential users the benefit of using various programs without having to pay fees. Agency users may decide a particular freeware utility offers certain advantages not found in any of the current enterprise software products, but will still be tied to the stipulations of the freeware end-user agreement. It is critical that the end-user agreement is understood and complied with as it often imposes certain restrictions such as "non-commercial use," meaning that it is not suitable for use by business and/or government agencies. There may be legal liabilities for any usage that violates the terms of the agreement.

6.1.2 Security

Vulnerabilities may exist in the underlying source code of the program. Embedded spyware/malware, Trojan horse programs, and macro execution are some examples of typical attack vectors that can be embedded within freeware and can often pass through anti-virus scans undetected. Because of the unknown nature of the underlying code in freeware software, allowing untested use of it in a production environment may pose an unacceptable security risk to Commonwealth assets and infrastructure.

6.1.3 Support

Since freeware software lacks guaranteed support from a software vendor or the type of support GNU/GPL-licensed software receives from the open source community, issue resolution may be difficult and time consuming. Freeware does not offer guarantees on functionality and cannot be validated to ensure that the end user knows exactly what they are obtaining. It is typically distributed without its source code, which prevents examination and modification by its users.

Compatibility issues may occur over time with other co-existing applications and there may be no way of resolving an issue other than trying to uninstall the program, which may or may not be easily accomplished. In addition, as newer versions of applications are rolled out through typical software lifecycles, upgrades to co-existing applications may need to take place to ensure compatibility. With freeware, users run the risk of not being able to obtain later versions when the product eventually becomes obsolete. The bottom line is that unsupported software can result in a costly interruption to service if it is too heavily depended upon or used in a way that creates interdependencies with other business applications.

Assuming approved deployment of freeware software, agencies are nonetheless solely responsible to review, assess risks in accordance with, and comply with all ITPs, including but not limited to the following requirements:

- Agencies are solely responsible to ensure that the use of freeware will not invalidate the terms as specified in the end-user agreement and that the product does not conflict with existing support agreements. Agencies granted approval to use a freeware application are to have their appropriate legal office review the terms of the product agreement to ensure they are acceptable to the commonwealth.

- Agencies are responsible for support and inventory control of freeware products. Freeware products to be used in production are to be tested and validated in a development environment to ensure security and quality control.

6.2 Open Source Software (OSS)

6.2.1 Usage

The license agreement must be reviewed by the agency's legal counsel along with the intended purpose of the OSS to assess the impact of the license provisions and to ensure the terms of the product agreement are acceptable to the commonwealth.

OSS prerequisite requirements must be reviewed. In some cases, OSS solutions use other open source solutions to implement functionality. As an example, some OSS may be maintained in a community repository (e.g. GitHub) 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.

6.2.2 Security

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 propriety 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.

6.2.3 Support

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. 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.

Integration and interoperability issues also need to be addressed when evaluating an OSS 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.

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.

Assuming approved deployment of open source software, agencies are nonetheless solely responsible to review, assess risks in accordance with, and comply with all ITPs, including but not limited to the following requirements:

- 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.
- Agencies are responsible to continually keep abreast of, and alert their legal offices to, the most up-to-date terms of agreements and other associated policies provided by licensors of OSS products.

6.3 Software as a Service (SaaS)

6.3.1 Usage

While SaaS is not licensed software, a service agreement is usually the vehicle for establishing user rights and restrictions. The agreement defines the services to be provided, contract term and renewal process, and the associated costs and/or subscription fees.

Agencies must understand what is covered by their agreement costs/fees such as setup and configuration services, customizations, integrations, providing access to previous or most current version of the product, training, allowable devices, usage (per device/user) fees and any termination fees. Data ownership must also be defined specifying how the vendor may or may not use the agency's data.

6.3.2 Security

Since the agency is dependent on the security mechanisms implemented by the hosting vendor, agencies must review and determine if the mechanisms provide adequate protection of their data and the functionality of the software. Robust authentication/authorization procedures and data encryption techniques must be in place to protect against unauthorized access to information. The vendor must have (and be regularly audited for) appropriate procedures to prevent (and address) data breaches and disaster recovery requirements, including periodic backup and recovery testing activities.

6.3.3 Support

Usage of a subscription-based service requires the agency to continue payments no matter the level of service provided by the hosting vendor unless appropriate service level requirements provide otherwise. Service level agreements (SLAs) must be established to define service availability and non-availability periods, acceptable performance levels, problem reporting/resolution/escalation processes and timeframes, data loss/damage/compromise prevention, fee credits for SLA breaches, and termination rights.

Upon termination, the agency must have a transition plan in place to ensure continuity of service to their users. They must ensure their data is returned in an agreed upon format or destroyed within the specified period of time defined in the SLAs.

7. Responsibilities

Commonwealth Agencies:

- Agencies considering the use of any of these software options are to ensure the technology solution is selected based on best value after careful consideration of all possible alternatives.
- Agencies are solely responsible to ensure that the installation and use of any of these software options will not invalidate the terms as specified in the license and/or agreement and that the product does not conflict with existing support agreements.
- Agencies are responsible for support and inventory control of software. These products to be used in production are to be tested and validated in a development environment to ensure security and quality control.
- Agencies must ensure proper disposal of these software options to prevent unauthorized use of licenses.
- Agencies are responsible for auditing installation, usage, copying and disposal of these software options to ensure compliance with applicable licensing/usage requirements.
- Agencies must ensure software licensing is addressed as part of education and awareness programs.
- Agencies are to adhere to Commonwealth standards for applying security related patches to these products. See ITP-SYM006 *Desktop and Server Software Patching Policy* for detailed information.
- Agencies are to give first preference to software listed as a current product standard in any of the existing Office of Administration/Office for Information Technology (OA/OIT) Information Technology Policies.

8. Related ITPs/Other References

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 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-SFT000 – *Software Development Life Cycle*
- ITP-SYM006 - *Desktop and Server Software Patching Policy*

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. Publication Version Control

It is the 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.

11. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

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

Version	Date	Purpose of Revision
Original	02/22/2017	Base Document Moved to Software domain from Application, including ITP number change Merged ITP-APP020 *Open Source Software*, ITP-APP033 *Use of Freeware Policy* into ITP Added additional guidance to Policy and Agency Responsibilities sections Inclusion of Software-as-a-Service (SaaS) language (temporary)