pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth IT Resources Patching Policy

ITP Number	**Effective Date**
ITP-SYM006	November 20, 2009
Category	**Supersedes**
Systems Management	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	January 2018

1. Purpose

This Information Technology Policy (ITP) defines the policy for timely application of software patches, and the methodology that will be used to monitor all IT Resources in the Commonwealth to ensure policy compliance.

2. Scope

This Information Technology Policy 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. Definitions

3.1 IT Resources: Include, but are not limited to, the staff, software, hardware, systems, services, tools, plans, data, and related training materials and documentation that in combination support business activities.

3.2 Server and Desktop Systems: Applies to all Commonwealth-associated platforms and infrastructure utilized to run and access IT resources. This includes the software (e.g. operating systems) and the hardware (e.g. routers, switches, etc.).

3.3 US-CERT: United States Computer Emergency Readiness Team tasked with providing cybersecurity resources and notifications for information security officers.

4. Policy

In an effort to better secure the Commonwealth network, computing infrastructure and user data, all server and desktop systems are to be kept up-to-date with service packs and security patches in accordance with the direction provided in this policy.

Service Packs:

When a software publisher releases a new service pack or similar major update for their software and / or firmware, such as operating system service packs and office suite application service packs, agencies are to deploy the service pack within six months of the release date. The six (6) month window provides a sufficient time during which the software upgrade can be fully tested and subsequently deployed before support for the previous service pack level ends.

New Software and Operation Systems:

Agencies shall coordinate with the Office of Administration, Office for Information Technology (OA/OIT) regarding the upgrade/deployment of new operating system software revisions. OA/OIT may direct at times the installation of entirely new software, if deemed critical by the Enterprise Information Security Office (EISO).

Security Patching

Microsoft OS and Microsoft, Java, and Adobe software patches

The EISO maintains the list of Microsoft operating system (OS) security patches and their Commonwealth-assigned severity ratings at https://itcentral.pa.gov/Security/Pages/default.aspx. In some cases, the security patch may not carry the same severity rating that the software publisher has assigned. In most cases, the EISO will send out an advance notification informing IT staff of upcoming patches and their corresponding severity levels. Contact the EISO at ra-ciso@pa.gov to determine the person at the agency who is on the notification list.

Non-Microsoft patches (AIX, Mainframe OS, Linux, network hardware OS etc.)

The policy is predicated upon preventative risk mitigation. Security patches for this category of systems and software shall be reviewed by appropriate agency administration teams and assessed accordingly.

At a minimum, agencies are responsible for monitoring patch recommendations provided by applicable software manufacturers and third-party entities such as the US-CERT. Agencies are responsible for applying system patches in accordance with such recommendations and best practices.

Agencies shall have a documented security patch schedule defining a definitive patch schedule for each platform. (e.g. AIX – Bi-annually, Mainframe – Quarterly)

Agencies shall have a monthly rollup and communication of announced security patches. This should be reviewed monthly to determine if the patch should deviate from the documented normal patching schedule.

Managing Portable Devices

All smartphones and non-Microsoft mobile devices (i.e. tablets) are not in scope of this policy. Agencies are to devise a methodology to apply patches to devices that do not routinely connect to the enterprise network. Refer to ITP-SEC035 *Mobile Device Security Policy* for guidance on mobile devices (e.g. iOS, Android).

Critical Patches

Critical (i.e. Heartbleed) type security patches shall be dealt with on an ad-hoc basis as determined by OA, agency, and external supplier security officers.

Active Outbreaks

If there is an active outbreak that uses an exploit patched in a security patch, testing may be foregone and OA/OIT may direct the agency to immediately deploy the patch to all systems. If a quarantine is required, at the discretion of the Commonwealth Chief Information Officer (CIO) in coordination with the Commonwealth Chief Information Security Officer (CISO), Commonwealth Chief Technology Officer (CTO), the impacted agency's CIO or designee, and agency Information Security Officer (ISO), the agency may be disconnected from the Commonwealth network until the outbreak is resolved.

Security Patching Schedule

The Commonwealth-defined severity levels, along with maximum timelines for deployment for each severity rating are listed in the following Security Patching Matrix. Agencies are to use the following Security Patching Matrix to determine the appropriate patching schedule.

OPD-SYM006A *Agency IT Resources Patching Schedule* is for internal agency use, is optional, and may be modified as needed. It is recommended that agencies develop a standardized internal patching policy aligned with this policy and OPD-SYM006A.

Security Patching Matrix

Technology Category	Critical Rating	Important Rating	Moderate Rating	Agency Schedule Required
Microsoft software	• Testing: Immediate • Deployment: 5 business days	• Testing: 5 business days • Deployment: 10 business days	• Testing: 10 business days • Deployment: 15 business days	No
Oracle software	• Testing: Immediate • Deployment: 5 business days	• Testing: 5 business days • Deployment: 10 business days	• Testing: 10 business days • Deployment: 15 business days	No
Adobe software	• Testing: Immediate • Deployment: 5 business days	• Testing: 5 business days • Deployment: 10 business days	• Testing: 10 business days • Deployment: 15 business days	No
AIX	• Testing: Immediate • Deployment: Agency Schedule	Agency Schedule	Agency Schedule	Yes
Mainframe OS	• Testing: Immediate	Agency Schedule	Agency Schedule	Yes

	• Deployment: Agency Schedule			
Linux OS	• Testing: Immediate • Deployment: Agency Schedule	Agency Schedule	Agency Schedule	Yes
Network hardware firmware/OS	• Testing: Immediate • Deployment: Agency Schedule	Agency Schedule	Agency Schedule	Yes
Other technologies (software and firmware)	• Testing: Immediate • Deployment: Agency Schedule	Agency Schedule	Agency Schedule	Yes

5. Responsibilities

5.1 The Office of Administration, Office for Information Technology is to utilize systems management server (SMS) and other reporting mechanisms to monitor the enterprise computing resources and ensure that current software, service pack, and patch levels defined in the above policy are in place across the Commonwealth.

5.2 Commonwealth agencies are to designate contacts responsible for patching all applicable systems or computing resources as dictated in this policy within that agency.

6. 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

- OPD-SYM006A - *Agency IT Resources Patching Schedule*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC001 – *Enterprise Host Security Software Suite Standards and Policy*
- ITP-SEC021 – *Security Information and Event Management Policy*
- ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*
- ITP-SEC035 – *Mobile Device Security Policy*
- US-CERT - https://www.us-cert.gov

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. 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.

9. 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	11/20/2009	Base Document
Revision	12/20/2010	ITP Refresh
Revision	04/10/2015	ITP Refresh
Revision	01/04/2017	ITP Reformat ITP title change Add language clarifying non-Microsoft patching Add Definitions and References sections General revisions to provide clarity Added supplemental OPD-SYM006A *Agency IT Resources Patching Schedule* Created a Security Patching Matrix for better viewing Clarified Active Outbreak authority to quarantine