**Information Technology Policy**
**Commonwealth of Pennsylvania**
**Governor's Office of Administration / Office for Information Technology**

| | | |
|---|---|---|
| **ITP Number:** | **ITP-SYM006** | |
| **ITP Title:** | **Desktop and Server Software Patching Policy** | |
| **Issued by:** | **Deputy Secretary for Information Technology** | |
| **Date Issued: November 20, 2009** | **Date Revised: December 20, 2010** | |
| | | |
| **Domain:** | **Systems Management** | |
| **Discipline:** | **Configuration Management** | |
| **Technology Area:** | **Patch Management** | |
| | | |
| **Revision History Date:** | **Description:** | |
| **12/20/2010** | **ITP Refresh** | |


## Abstract:
In an effort to better secure the Commonwealth network and computing infrastructure, all server and desktop platforms are to be kept up-to-date with service packs and security patches. Recent virus outbreaks have brought some agencies to a standstill, prevented access to the Internet, and in some cases caused loss of revenue to the Commonwealth from outages. This Information Technology Policy (ITP) defines the policy for timely application of software patches, and the methodology that will be used to monitor all desktop and server resources in the Commonwealth to ensure policy compliance.

This policy applies to all software on Commonwealth computing resources, including Microsoft and non-Microsoft software in the Windows platform, and UNIX and Linux platforms.


## General:
This 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 policy to ensure that application of software patches is accomplished in a timely manner across the enterprise.

The Bureau of Enterprise Architecture (EA) updated and refined software patching standards for the Commonwealth. EA evaluated the patch management systems currently deployed within the Commonwealth, past patch deployment timelines, previous experience of Commonwealth assets not being patched in a timely manner, and other relevant business and technical criteria to support their recommendations. This policy covers all software in use on Commonwealth information technology (IT) hardware assets, including operating systems, regardless of platform.

## Policy:
Unsupported Software:
In the Commonwealth, unsupported software is defined as software no longer supported by the vendor that produced it.

> **NOTE:** A product being supported by a vendor does not mean that the Commonwealth also supports the product at an enterprise level.

Such software is not to be installed on Commonwealth production hardware. This includes operating systems and service packs or updates for these operating systems. While a vendor may support a certain operating system or software package, they may only specifically support that OS

of software at certain service pack or patch levels. In general, vendors also provide support retirement dates well in advance.

Service Packs:
When a vendor releases a new major update/service pack for his/her software, including operating systems and office suite applications, agencies are to deploy the service pack within six months of the release date. The six-month windows provides a large cushion during which the software upgrade can be fully tested and subsequently deployed before support for the previous service pack level ends. This may also include entirely new versions of software, if deemed critical by the Chief Information Security Office (i.e., a new version of antivirus software). This policy does not include a new operating system (i.e., Windows XP should not be upgraded to Windows Vista).

## Security Patches:

**Microsoft patches**: Typically, Microsoft releases security patches on the second Tuesday of every month. The office of the CISO maintains the list of security patches and their Commonwealth-assigned severity ratings at http://www.cybersecurity.state.pa.us. In some cases, the security patch may not carry the same severity rating that Microsoft has assigned. In most cases, the CISO will send out an advance notification informing IT staff of upcoming patches, and their corresponding severity levels. Contact the CISO at ra-ciso@state.pa.us to determine the person at the agency who is on the notification list.

The Commonwealth-defined severity levels are listed below, along with maximum timelines for deployment for each severity rating:

| Severity Rating | Test and begin deployment | Deadline for complete deployment |
|---|---|---|
| CRITICAL | Immediate | 5 business days |
| IMPORTANT | Within 5 days | 15 business days |
| MODERATE | Within 10 days | 25 business days |

Non-Microsoft software patches are to be deployed at the same schedule as above, with the CISO setting the start date for deployment (similar to the Microsoft "patch Tuesday").

> **NOTE:** If there is an active outbreak of a virus that uses an exploit patched in a security patch, testing may be foregone, and Office of Administration/Office for Information Technology (OA/OIT) may direct the agency to immediately deploy the patch to all systems. In addition, the agency may be disconnected from the MAN until the outbreak is resolved.

Managing Mobile Devices (Laptops, etc.)
Agencies are to devise a methodology to apply patches to devices that do not routinely connect to the enterprise network. OA/OIT feels that the security of the enterprise is far too important to modify this policy because laptop users do not connect to the network often enough to stay properly patched. There have been several instances in the past where Commonwealth business has been disrupted due to a user reconnecting to the network with an unpatched device.

Monitoring and Enforcement Policy:

- OIT 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.
- Agencies are to designate contacts who are to be responsible for patching all servers and desktops within that agency.

## Refresh Schedule:

All standards identified in this ITP are subject to periodic review and possible revision, or upon request by the Enterprise Architecture Standards Committee (EASC).

## 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. Contact your agency CoP Planner for further details or assistance.

## Questions:

Questions regarding this policy are to be directed to ra-itcentral@pa.gov.