Information Technology Policy

Commonwealth IT Resources Patching Policy

Number ITP-SEC041	**Effective Date** November 20, 2009
Category Security	**Supersedes** ITP-SYM006
Contact RA-ITCentral@pa.gov	**Scheduled Review** May 2023

1. Purpose

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

2. Scope

This ITP applies to all departments, offices, 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 as outlined in the Responsibilities section.

3. Definitions

3.1 Appliance: A device that consists of hardware and software packaged together to accomplish a specific function(s) or provide a predefined service.

3.2 Network Device: A hardware component of the network infrastructure such as, routers, switches, wireless access points, etc.

3.3 Peripheral Device: An auxiliary device that connects to and works with a computer and is typically used to input information into it or get information out of it.

4. Policy

In an effort to better secure the Commonwealth network, computing infrastructure and data, IT resources including, but not limited to, Server and Desktop Systems, Network Devices, Peripheral Devices, Appliances, and Mobile Devices shall be kept up-to-date with cumulative updates and security patches in accordance with the direction provided in this policy and schedules contained in OPD-SEC041B *Commonwealth IT Resources Patching Schedule*.

4.1 Security Patching

The Enterprise Information Security Office (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 the event the EISO assigns a higher severity rating than the manufacturer, the severity rating assigned by the EISO shall be used. 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. Additional information from Microsoft regarding security updates can be found at https://msrc.microsoft.com/update-guide.

Security patches for Non-Microsoft 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 that defines 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.

4.2 Security Patching Schedule

The Commonwealth-defined severity levels, along with maximum timelines for deployment for each severity rating are listed in supplemental document OPD-SEC041B *Commonwealth IT Resources Patching Schedule*. Agencies are to use OPD-SEC041B to determine the appropriate patching schedule.

OPD-SEC041A *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-SEC041A.

4.3 New Software and Operating Systems

Agencies shall coordinate with the Office of Administration, Office for Information Technology (OA/OIT) regarding the upgrade and/or deployment of new operating system software revisions in accordance with ITP-PLT005 *Server Operating System Policy*. OA/OIT may direct the installation of entirely new software, if deemed critical by the EISO.

4.4 Managing Portable Devices

All smartphones and non-Microsoft mobile devices (i.e., tablets) are not in scope of this policy. Agencies shall 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).

4.5 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.

4.6 Active Outbreaks

If there is an urgent vulnerability that is rated critical or high on the Common Vulnerabilities and Exposures list (CVE) or an active outbreak that uses an exploit patched in a security patch, testing may be foregone, and OA/IT 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), and the impacted agency's CIO, ISO, and CTO, the agency may be disconnected from the Commonwealth network until the outbreak is resolved. Notification of a probable or imminent quarantine or disconnection from the Commonwealth network shall be made to the affected agency CIO, ISO, and CTO as soon as practical and before the actual disconnection occurs.

5. Responsibilities

5.1 Agencies shall:

- Designate contacts responsible for patching all applicable systems or computing resources as dictated in this policy within that agency.
- Use OPD-SEC041B to determine the appropriate patching schedule for the systems and software covered in that document.
- Have a documented security patch schedule defining a definitive patch schedule for each platform.
- Monitor patch recommendations provided by applicable software manufacturers and third-party entities and apply system patches in accordance with such recommendations and best practices.

5.2 The Office of Administration, Office for Information Technology (OA/OIT) shall:

- Maintain a list of Microsoft operating system security patches and their Commonwealth-assigned severity ratings and communicate this information to applicable IT staff.
- 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.

5.3 *Third*-party vendors, licensors, contractors, or suppliers providing services to the Commonwealth shall ensure patches are applied to all systems or computing resources consistent with the requirements defined in the above policy.

6. 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*
- OPD-SEC041A *Agency IT Resources Patching Schedule*
- OPD-SEC041B Commonwealth IT Resource Patching Schedule
- ITP-PLT005 *Server Operating System Policy*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC001 *Enterprise Host Security Software 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 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 are to be directed to RA-ITCentral@pa.gov.

9. 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 is to 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	11/20/2009	Base Document	N/A
Revision	12/20/2010	ITP Refresh	N/A
Revision	04/10/2015	ITP Refresh	N/A
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	N/A
Revision	04/28/2022	• Changing Domain to Security • Creating a new supplement document OPD-SEC041B • Patching schedules moved from policy to new confidential supplemental document OPD-SEC041B • Updated rating for Critical deployments per ETSO guidance • Third-party vendors added to Scope and Responsibilities Section • Definitions added/removed where necessary	Revised IT Policy Redline <04/28/2022>