Information Technology Policy
IT Resources Patching Policy

Number ITP-SEC041	**Effective Date** November 20, 2009
Category Security	**Supersedes** ITP-SYM006
Contact RA-ITCentral@pa.gov	**Scheduled Review** December 2024

1. Purpose

This Information Technology Policy (ITP) sets forth the requirements for the timely application of security 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 and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Definitions

Firmware: Software program or set of instructions programmed on the flash read-only memory (ROM) of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.

Middleware: Agency installed software, or software installed on behalf of the agency at their request (e.g., Oracle, Java, Tomcat, Telerik, Wordpress, etc.)

Software: A set of instructions, data, or programs used to operate computers and execute specific tasks. Software is a generic term utilized to refer to applications, scripts or programs that run on a device. (e.g., Microsoft Office, Firefox, etc.)

4. Policy

In an effort to better secure the Commonwealth network, computing infrastructure, data, and IT resources including, but not limited to, Server and Desktop Systems, Network Devices, Peripheral Devices, Appliances, and Mobile Devices, agencies shall

ensure the most recent cumulative updates and security patches are applied in accordance with this policy and the schedules contained in *OPD-SEC041B, IT Resources Patching Schedule (Authorized user access only)*.

The Enterprise Information Security Office (EISO) provides security patch information/updates, vendor severity ratings and in some instances Commonwealth severity ratings (when they vary from vendor) on the IT Central Security Services Page (*Authorized user access only*). In the event the EISO assigns a higher severity rating than the manufacturer, the severity rating assigned by the EISO shall be used. In addition to the information/updates provided by EISO, Agencies shall ensure that technology owners are monitoring vendor resources (e.g., email, website, etc.) for associated vulnerability announcements and patch updates for the Commonwealth IT resources which they support.

Notifications are sent to the Agency Information Security Officer (ISO). Agencies shall contact OA, EISO Notifications (RA-OAEISONOTIFICATIO@pa.gov) if there is an agency need for additional users to be added to the notification list.

To ensure agency patching is conducted in accordance with this policy, the Agency ISO is authorized to conduct compliance audits and provide guidance on associated risks and vulnerabilities.

4.1 Security Patching Requirements

The severity levels, along with maximum timelines for deployment for each severity rating, are listed in supplemental document *OPD-SEC041B, IT Resources Patching Schedule (Authorized user access only)*. Agencies shall use this information and *OPD-SEC041B* to determine the appropriate patching schedule.

To ensure consistent patching of Commonwealth IT Resources, agencies shall:

- Develop a standardized internal patching policy aligned with this policy and *OPD-SEC041A, Agency IT Resources Patching Schedule*.
    - Ensure patching timelines are no less stringent than those established within this policy. *OPD-SEC041A* is an optional template that may be utilized and modified as needed.
- Document a security patch schedule including a definitive patch schedule for each platform. (e.g., AIX – Bi-annually, Mainframe – Quarterly)
- Plan and implement monthly rollup patching and communication of announced security patches to impacted or affected entities. This plan should be reviewed monthly to determine if the patch should deviate from the documented normal patching schedule.
- Monitor patch recommendations provided by applicable software manufacturers, third-party entities such as the US-CERT, and apply system patches in accordance with such recommendations and best practices.

4.2 Network Devices and Security Appliances

Agencies shall ensure network devices and security appliances are upgraded to address any known vulnerabilities. Refer to *OPD-SEC041B* for guidance on the patching of these devices.

4.3 Internet of Things (IoT) and Supervisory Control and Data Acquisition (SCADA)

Agencies shall ensure IoT and SCADA devices are upgraded to address any known vulnerabilities. Refer to *OPD-SEC041B* for guidance on the patching of these devices.

4.4 New Firmware, Middleware, Software, and Operating Systems

Agencies shall coordinate with the EISO at RA-OAEISOVulnMgmt@pa.gov regarding the upgrade and/or deployment of new firmware, middleware, software, and operating system software revisions in accordance with *ITP-PLT017, Desktop and Laptop Operating System Standards* and *ITP-PLT005, Server Operating System Policy*. OA/IT may direct the installation of entirely new software, if deemed critical by the EISO.

4.5 Managing Mobile Devices

Authorized users who are issued Mobile Devices are responsible for monitoring for and ensuring routine security updates are installed within 10 days of the updates release. OA will provide notification to end users of the availability of critical security updates for Mobile Devices which require immediate installation to the device.

Agencies are responsible for ensuring users are installing updates in a timely manner to provide for the adequate protection of Commonwealth data. The installation of updates on Mobile Devices requires a wi-fi connection. As per policy, this shall be a non-public connection, users should refer to *ITP-SEC035, Mobile Device Security Policy* for policy guidance on mobile devices in regard to the restriction on connections to public wi-fi.

4.6 Zero-Day/Actively Exploited Critical Vulnerabilities

Zero-day/actively exploited critical vulnerabilities (i.e., Heartbleed) shall be dealt with on an ad-hoc basis as determined by OA, agency, and external supplier ISOs. This patching will be expected to be completed on an expedited schedule upon release of vendor supplied patch or workaround, while maintaining the general guidelines for patching (testing prior to production, where possible). Refer to *OPD-SEC041B* for further guidance regarding emergency patching and mitigation measures.

4.7 Active Outbreaks

For systems or networks in which an active outbreak has been found, and a quarantine is required, the agency may be disconnected from the Commonwealth network until the outbreak is resolved. This may be 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. 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 IT resources as

dictated in this policy within that agency.
- Use OPD-SEC041B to determine the appropriate patching schedule for the IT resources 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 ensure system patches are applied in accordance with such recommendations and best practices.

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

Ensure security patches are applied in accordance with this policy to:
- Any systems connecting to the Commonwealth network.
- Any systems or applications that are hosting or transmitting Commonwealth data.

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 (Authorized user access only)*
- *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*
- *ITP-SYM010, Enterprise Services Maintenance Scheduling*

- *US-CERT (CISA) Homepage*

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 shall 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	N/A
Revision	12/01/2023	• Updated Scope based on connection to Commonwealth Network. • Replaced definitions with links to glossary where applicable. • Added definitions for Firmware, Middleware and Software. • Removed section heading for 4.1 Security Patching. Previous language rolled into general Section 4. Policy.	Revised IT Policy Redline <12/01/2023>

Version	Date	Purpose of Revision	Redline Link
		• Policy language regarding distribution of patch updates/information updated added language for agency monitoring of vendor resources for updates. • Updated contact email to for additional notifications. • Added statement authorizing Agency ISO to conduct audit compliance and provide guidance on risks/vulnerabilities. • New section 4.1 Security Patching Requirements added requirement to monitor and apply patch recommendations provided by applicable software manufacturers and 3rd parties. • Added 4.2 Network Devices & Security Appliances, 4.3 IoT and SCADA, 4.4 New Firmware, Middleware, Software, and Operating Systems, 4.5 Managing Mobile Devices, 4.6 Zero-Day/Actively Exploited Critical Vulnerabilities. • Sections 4.2 and 4.3 populated with language to reference OPD-SEC041B for guidance. • Section 4.4 reference added to ITP-PLT017. • Section 4.5 Added requirement for patching of mobile devices to within 10 days of update release. OA will provide notification of critical updates. Sets requirement for agencies to ensure users are installing updates, wi-fi is utilized to install updates and reminder that public wi-fi is restricted. • Section 4.6 Critical patches updated to Zero-day/actively exploited critical vulnerabilities. Overview of patching requirement updated, and reference added to OPD-SEC041B. • Section 4.7 language updated to allow the disconnection of a system or network which is found to have an active outbreak. • Third party vendor requirements updated. • Removed “Commonwealth” from policy title. • Added links to supporting documents.	