IT Resources Patching Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
June 30, 2026

Supersedes:
ITP-SEC041

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. 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.

3. Scope

This policy applies to all offices, departments, 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 policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

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 the *IT Resources Patching Schedule Procedure*.

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 a 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 *IT Resources Patching Schedule Procedure*. Agencies shall use this information and the Procedure 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 the *Agency IT Resources Patching Schedule Procedure.*
    - Ensure patching timelines are no less stringent than those established within this policy. The *Agency IT Resources Patching Schedule Procedure* 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 the *IT Resources Patching Schedule Procedure* 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 the *IT Resources Patching Schedule Procedure* 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 the *Desktop and Laptop Operating System Standard* and the *Server Operating System Standard*. 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 the *Mobile Device 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 the *IT Resources Patching Schedule Procedure* 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. Contact

Questions or comments may be directed via email to OA, IT Policy

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document