

Patching Policy

Note to the Leader

This is a draft template the you can customize to suit your organization. The policy below contains the suggested rules. Some of these may not be practical for every organization and you should get input from all department heads before finalizing.

[[ORG]] – Patching Policy

Purpose: Prompt and complete patching of systems is critical to defending against attacks. The vast majority of cyber attacks target systems that have known vulnerabilities, and haven't been patched. Your laptop, your personal cell phone, and the servers [[ORG]] use must all be patched against the latest security vulnerabilities in order to protect our data, systems, and networks.

Scope: this policy applies to all of [[ORG]] employees and contractors accessing [[ORG]] systems, network and data, whether from [[ORG's]] devices or personal device.

Patching Definition: A patch is a software update designed to fix security vulnerabilities in existing computer systems or applications. Patching is the process of downloading and installing the patches.

Policy

While everyone plays a role in keeping [[ORG]] patched against security vulnerabilities, you will have different responsibilities, depending on your organizational function.

1. All employees:
 - A. Enable auto-update on all your devices, including personal devices, such as cell phones and tablets that connects to [[ORGs]] network. This action includes operating system auto-update (e.g.: Windows, OS X, iOS, Android, etc.). If you have questions on how to enable these features, please ask the Leader.

- B.** Don't ignore the auto-update notifications. Once prompted, install the update within 24 hours. If you are unable to do so, please notify the Leader.
- C.** When selecting software or cloud services, favor vendors that have robust and effective policies and procedures around patching.

2. Cyber leader and/or IT Staff

- A.** Ensure that patches are installed, or installed for testing, within 72 hours of patch release for servers and infrastructure systems (such as routers).
- B.** Subscribe to all mailing list/notification systems of exiting vendors to ensure you receive notifications of patches.
- C.** In the case of critical systems or software, if applicable test updates/patches before they are deployed.
- D.** On a quarterly basis, scan and monitor all devices to verify that all appropriate released patches have been installed.

Signatures

Date Approved

Date Last Modified

Approved By

Modified By

To access the full Cyber Readiness Program, visit www.cyberreadinessinstitute.org.