IT Patch Management Policy
TEC 15.0

Office of Information Technology

Institutional Type: Operational
Applies to: Office of Information Technology Staff Members

POLICY DATES

Issued: 12/11/2019
Revised Last: 4/07/2023
Edited by: Tina Stuchell
Reviewed: 4/07/2023

This document establishes the patch management policy for the University of Mount Union. This policy defines requirements for the management of information security vulnerabilities and the notification, testing, and installation of security-related patches on devices connected to the University network. This policy applies to all information systems and information resources owned or operated by or on behalf of the University.

Mount Union is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT vulnerabilities. A compromised computer threatens the integrity of the network and all computers connected to it. Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Proactively managing vulnerabilities will reduce or eliminate the potential for exploitation and involved inconsiderably less time and effort than responding after exploitation has occurred.

The purpose of this policy is to ensure that all University-owned devices are proactively managed and patched with appropriate security updates.

Definitions

Term	Definition
Patch Management	Refers to a formal process for applying patches to systems and resources in order to protect against vulnerabilities.
IT	Information Technology
Change Management Log Report	Log that is maintained by IT Staff Members related to changes in the IT Environment, including recording of patches.
Patch	Software or firmware update provided by the application or system vendor.
Third-Party Vendors	Third-Party Vendors are vendors that the institution does business with. In the case of patch management, these third-party vendors are software and hardware vendors in which the institution uses their product for business purposes.

Policy Details

This policy provides the processes and guidelines necessary to:

- Maintain the integrity of network systems and data by applying the latest operating system and application security updates/patches in a timely manner.
- Establish a baseline methodology and timeframe for patching and confirming patch management compliance.

Desktops, laptops, servers, applications, network devices represent access points to sensitive and confidential university data, as well as access to technology resources and services. Ensuring updates and patches are distributed and implemented in a timely manner is essential to maintain system stability and mitigate malware, exploitation, and security threats.

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the Mount Union network shall be regularly maintained by

applying critical security patches within thirty (30) days after release by the vendor. Other patches that are medium/high severity or for non-critical systems must be rolled out within ninety (90) calendar days. Any low priority patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.

In the case where patches cannot follow the aforementioned schedule, a document must be produced explaining why the patch must be deferred. Permissible deferrals may include a lack of appropriate change windows within the appropriate timeframe or a conflict with other critical changes scheduled at the time. Any patches which are to be deferred longer than the scheduled timeframe must be approved by the Director of IT for Security or Chief Information Officer or his/her assignee. All deferred patches must be reviewed at least quarterly.

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data.

On occasion a software vendor will release a highly critical security patch outside of their normal release cycle. The usual reason for the release of an out-of-band patch is the appearance of an unexpected, widespread, destructive exploit that will likely affect a large number of users. In the event of a published out of band patch, IT will expedite the validation process. Once validated, users will have one business day to install and reboot their machine to apply the patch. IT will communicate appropriately regarding any critical patches outside the normal release cycle.

All University-owned endpoints are to be critical operating systems and key application patches installed within 30 days of *release from* the vendor. This policy applies to all Enterprise Servers which are owned by the University. It also applies to University-issued endpoints bound to Active Directory (AD).

Third-Party Vendor Patch Management

Third-party patch management is the process of installing patches to third-party applications (software or hardware/firmware), that are installed on premise or in the cloud for use by the institution. Patch management addresses bugs or vulnerabilities in the software or firmware. Third-party patching is critical for the security of our organization that assists us in preventing a data breach.

The third-party software/application patch management process is essential. Most institution third party vendors in which the institution uses their software that is in the cloud as a Software As A Service (SaaS) adheres to a patch release schedule and applies critical patches immediately when a vulnerability is discovered. The Administrative Systems area of Information Technology records the patch schedule of all software related to the use in administrative offices that are SaaS and on premise. The Technical Services area of Information Technology oversees the patch schedule on applications or firmware that they oversee.

Procedures

Software vendors release security patches on a regular schedule. Applicable patches will be tested and validated by IT prior to deployment to campus. Once validated, IT will schedule and deploy validated patches to end points on a monthly basis. Communication to campus regarding deployed security patches will be done through Campus Communications.

A system reboot is required to successfully install most security patches. Until the reboot occurs, the computer remains vulnerable to attacks which the installed patch protects against. IT understands the impact all ill-timed reboot can have on the campus community and user productivity. In order to provide the University community with as much flexibility as possible, security updates will be deployed after regular hours on servers, devices and hardware when possible. End User machine updates take place on next reboot by end user, typically. Typical normal down time for patches to be applied at the University is generally Thursday mornings between 1:00am and 5:00am.
Third-party vendor software and firmware patch management is overseen by administrative systems and technical services within the Office of Information Technology. A log is kept recording the patch management activity per application and/or firmware that the institution uses for patch management. IT is looking at implementing Patch my PC for window

Applies to: Information Technology Staff Members

machines and JAMF for Macs for an automatic way to record patch management for local machines. SaaS applications are documented manually.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology (Technical Services, Director of IT for security & CIO)	Update of policy

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330-823-2854	IT@mountunion.edu

History

This policy was established in 2019 part of GLBA compliancy.
All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.

Issued: 12/11/19

Revised: 4/07/2023

Edited: Tina Stuchell

Reviewed: 04/07/2023