THE UNIVERSITY OF ARIZONA
R. KEN COIT COLLEGE OF PHARMACY
Information Technology

Workstation/Server Patch Management Policy

Purpose of document: **The document addresses management of patching activities to protect College of Pharmacy assets**

Office/department responsible: **College of Pharmacy, Office of Information Technology**

Document classification level: **PUBLIC**

Effective Policy Date: **March 2022**

Patch Management Policy

Policy Statement

COP digital assets must be protected and listed by a rigid and reasonable patching activities. Vulnerabilities should be patched adequately. COP has the right to protect its assets and ensure its compliance.

Reason for Policy/Purpose

The purpose of this patch management policy is to enable COP IT to:

Ensure community is fully aware of the requisite security needed to patch a digital asset and describe the patching controls and constraints to minimize information security risks affecting COP digital assets.

Who Needs to Know This Policy?

All College of Pharmacy users that have/use a university purchased computer or device.

Web Address for this Policy

https://it.pharmacy.arizona.edu/policies-and-guidance

Contacts

Responsible College Official: Rick Schnellmann - Dean - Pharmacy Administration

Responsible College IT Official: Anthony Schlak - Director, Information Technology

Responsible University Office: College of Pharmacy, Office of Information Technology

If you have any questions on the policy, you may send an e-mail to helpdesk@pharmacy.arizona.edu

Definitions

Term	Definition as it relates to this policy
Vulnerability	Weakness in system or application that allows attackers or abusers to take advantage and affect the system/application confidentiality, integrity, or availability.
Patch	Is a code or software update that covers/solves a certain vulnerability
Digital Asset	Server, PC, Laptop, Printer, Network device, storage device……etc.
Domain	A domain is a computer network in which all user accounts, computers, printers, and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers.
Domain Joined Devices	Devices that are joined to the **pharmacy.pharmacy.arizona.edu** domain. Devices that can only be logged into with a College of Pharmacy credentials.
Non-Domain Joined Devices	Devices that are not on the Pharmacy domain and have a local account to login.

Policy/Procedures

1. All COP digital assets, systems or services should be patched and updated against any security vulnerability.
2. The patching scope includes but not limited to: - operating system, applications, database systems, program components…etc.
3. All Information Systems shall be maintained to be patched continuously and as fast as possible.
4. This policy is considered a general patch management procedure and shall apply to all Information Systems, digital assets, or services by default.
5. Patching shall be performed during an authorized maintenance time window unless there is an urgent situation. System patches will be applied monthly on the third Saturday of the month from 7:00 PM – 7:00 AM MST.
6. To ensure that patches are properly applied user devices may be restarted to ensure patch effectiveness.
7. Critical system data shall be backed up prior to installation of new patches
8. Patching process is a joint responsibility of both system's administrator and application's administrator. They should work closely to ensure that.
9. In general cases, maximum tolerance time to have COP systems/services stay unpatched is 30 days (about 4 and a half weeks). According to vulnerability severity, Information Security will decide to shorten this tolerance time to minimize risk to COP assets and reputation.
10. Data domain trustees and data stewards are accountable for providing adequate support and maintenance time window to enable data custodians, systems, and application's administrators to patch the systems as needed.

    Data Domain Trustees = College of Pharmacy Information Technology Personnel

    Data Stewards = Anyone who adds, edits, or saves data on college devices.

Users' Managed Assets

1. Users managed assets like PCs and laptops…etc. should be patched by COP IT. User is not responsible for the patching process; however, users should adhere to IT and Information Security communications with regards to any associated responsibilities like bringing the device to campus/IT, restarting the machine, stop using certain software…. etc.
2. Some users' managed assets may have some extra administrative privileges that are granted to its users like the ability to install, uninstall programs/updates, these granted users are responsible to adhere to IT and Information Security constrains and communications with regards to patching and to execute them as needed. Violators will be revoked their administrative privilege and disciplinary actions will be taken against them.
3. Users managed assets like PCs and laptops…etc. should be built and managed by COP IT. Upon initial set up, COP IT will install software for O365 Apps, Adobe Acrobat, Google Chrome, Mozilla Firefox, LogMeInResuce, Cisco AnyConnect VPN, Zoom, and Sophos Central. COP will patch/manage the software and applications they install on the devices. Any software or applications installed by the user; COP IT does not assume responsibility for.

Users' Non-Managed Assets

1. Users that have assets purchased with university funds such as PCs, Laptops, Storage/Network Devices, or laboratory equipment that are unable-to join the College of Pharmacy Domain because they are incompatible with Antivirus software or being joined to a domain network are subject to vulnerabilities. Non-Domain Joined assets cannot be monitored via PDQ Inventory or have group policy objects pushed out to them. Users with local accounts and non-domain joined machines take responsibility for patching and keeping their digital assets up to date. COP IT does not take responsibility for patching or securing these devices.
2. COP IT does not assume responsibility for users' personal devices, i.e., laptops, pcs, etc. COP IT strongly recommends that the user install Antivirus and keep up with security patches.

Patch Management

COP IT oversees the patching process; progress reports and new patch releases should be delivered continuously. A formal and updated asset inventory will be kept and managed by College of Pharmacy IT.

Exceptions

Exceptions should be as minimum, if they exist, they should be approved by the Information Security Office and/or COP Information Technology Administration.

Enforcement

Any user found to have violated this policy (or part thereof) may be subject to disciplinary action. Including but not limited to termination of their College of Pharmacy user account and computer privileges. The College of Pharmacy Dean and Administration will determine the disciplinary action at time of event.

History/Revision Dates

Effective Date	Version #	Author	Description
March 15, 2022	1.0	Nic Altamirano Anthony Schlak	Initial version.

Next Review Date: TBD