Workstation/Server Patch Management Policy

Effective Policy Date: **May 30, 2023**

Patch Management Standard

Purpose of document: **The document addresses management of patching activities to protect Arizona Space Institute assets**

Office/department responsible: **Arizona Space Institute, Office of Information Technology**

Policy Statement

ASI digital assets must be protected and listed by rigid and reasonable patching activities. Vulnerabilities should be patched adequately. ASI is obligated to protect its assets and ensure their compliance.

Reason for Policy/Purpose

The purpose of this patch management policy is to enable ASI 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 ASI digital assets.

Who Needs to Know This Policy?

All Arizona Space Insititute users and building occupants that have/use a university purchased computer or device.

Web Address for this Policy

https://it.space.arizona.edu/compliance/policy-procedure-guidance

Contacts

Responsible College Official: Tim Swindle - Director – Arizona Space Institute

Responsible College IT Official: Nicolas Altamirano - Director, Information Technology

Responsible University Office: Arizona Space Institute, Office of Information Technology

If you have any questions on the policy, you may send an e-mail to ASI-IT@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 principles, 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 any University of Arizona domain, (i.e., bluecat.arizona.edu). Devices that can only be logged into with UA credentials.
Non-Domain Joined Devices	Devices that are not on a University of Arizona or Arizona Space Institute domain and have a local account to login.

Policy/Procedures

1. All ASI 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 at a minimum, monthly.
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 Friday 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 ASI 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 ASI 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. Notification of patches will be provided to users in advance.

    Data Domain Trustees = Arizona Space Institute Information Technology Personnel

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

Users' Managed Assets

1. Users managed assets like PCs and laptops…etc. should be patched by ASI 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 have their administrative privilege revoked and disciplinary actions will be taken against them.
3. Users managed assets like PCs and laptops…etc. should be built and managed by ASI IT. Upon initial set up, ASI IT will install software such as O365 Apps, Adobe Acrobat, Google Chrome, Mozilla Firefox, Cisco AnyConnect VPN, Zoom, and Sophos Antivirus. This list of software is non-inclusive and is subject to change. ASI will patch/manage the software and applications they install on the devices. ASI IT does not assume responsibility for any software or applications installed by the user.

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 UA or ASI 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. ***ASI IT does not take responsibility for patching or securing these devices.***
2. ASI IT does not assume responsibility for users' personal devices, i.e., laptops, pcs, etc. ASI IT strongly recommends that the user installs Antivirus and keeps up with security patches.
3. Personal devices connecting to ASI or UA information and data assets must have the following minimum controls. Time-based screen lock, device encryption, password/face/gesture lock, etc.

Patch Management

ASI 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 Arizona Space Institute IT.

Exceptions

Exceptions should be as minimum, if they exist, they should be approved by the University Information Security Office Governance, Risk, & Compliance (ISO GRC), Institute Director, and ASI 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 ASI user account and computer privileges. The ASI Director and Administration will determine the disciplinary action at time of event.

History/Revision Dates

Effective Date	Version #	Author	Description
May 30, 2022	1.0	Nic Altamirano	Initial version.

Next Review Date: 5/30/2024