SPACE INSTITUTE
Information Technology

Vulnerability Management Program

Effective Policy Date: May 30, 2023

Purpose of document: This document addresses the procedures and processes for conducting Network Vulnerability Scans on Arizona Space Institutes digital assets.

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

Policy Statement

Network attached ASI digital assets must be protected and listed by reasonable, but rigid vulnerability management processes. Vulnerabilities should be patched regularly while maintaining normal operating procedures. ASI is obligated to protect its assets and ensure their compliance.

Policy Purpose

The purpose of this vulnerability management policy is to enable ASI IT to:

Establish rules for the review, evaluation, application, and verification of network vulnerability scans conducted on ASI digital assets.

Who Needs to Know This Policy?

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

Contacts

Responsible University Official: Director – Arizona Space Institute

Responsible University IT Official: Director, Information Technology

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

If you have any questions on the procedure, you may send an e-mail to ASI-IT@arizona.edu

Web Address for this Policy

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

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.
Network attached Digital Asset	Server, PC, Laptop, Printer, storage, or any other device that is physically or wirelessly connected to the UA network.
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.

APPENDIX

Policy/Procedures

1. All ASI network attached digital assets, systems, or services should be scanned weekly on Thursday evenings to detect potential security vulnerabilities.
2. Vulnerability scans will be monitored every Friday by a member of the ASI IT team. A log of the monitoring process will be maintained and updated accordingly. As new vulnerabilities arise they will be mitigated as follows.
3. The vulnerability scans include but are not limited to common vulnerabilities such as – SSL/TLS Version, Operating System, Certificates, SNMP, open port checks, etc…
4. All vulnerabilities are weighted by the following severity levels: Critical, High, Medium, Low, and Info. Each vulnerability also includes a total number of instances (affected assets).
5. In order to lower the potential attack surface of ASI networks, vulnerability patching orders will be determined by severity and number of instances. For instance, twenty high severity findings create a wider attack surface and may be patched before one critical finding.

6. Vulnerability patching shall be performed to meet the University of Arizona's SLA time frames. Critical: 7 Days, High: 30 Days, Medium: 60 Days, Low: 180 Days.
7. According to vulnerability severity, Information Security may decide to shorten this tolerance time to minimize risk to ASI assets and reputation.
8. To ensure that patches are properly applied user devices may be restarted to ensure patch effectiveness.
9. Critical system data shall be backed up prior to configuration of vulnerability patches.
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 connected to a UASI network will be included in vulnerability scans by ASI IT. Users are not responsible for the patching process; however, they should adhere to IT and Information Security communications with regards to any associated responsibilities such as: scheduling time for vulnerability management patches, restarting the machine, updating certain software…. etc.
2. Users managed assets like PCs and laptops…etc. should be built and managed by ASI IT. Upon initial set up, ASI IT will join the device to a Domain that includes group policies objects that mitigate common vulnerabilities. These objects will be kept up to date by ASI IT and new policies may be created to patch future vulnerabilities. If the new policy has potential to interrupt the flow of research/business e.g., a restart is required, ASI IT will work with the individual managing the asset to streamline this process while maintaining network security.

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, are subject to vulnerabilities. Non-Domain Joined assets connected to the UA network will still be monitored via the Vulnerability Management Programs. However, these assets are still required to adhere to this policy. ASI IT will provide support when needed to patch known vulnerabilities but **does not take responsibility for patching or securing these devices.**
2. Users that do not work with ASI IT to patch these devices will be removed from the UA network until they are able to comply with the SLAs set forth by the University.
3. 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.

4. 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.
5. ASI IT will ensure network vulnerability scans are run on all ASI Managed Networks. ASI IT is not responsible for network assets located in buildings/location not managed by ASI. ASI Users/Building occupants with equipment connected to these networks wishing to include those devices in Network Vulnerability Programs will need to work with the IT department responsible for those networks.

Vulnerability Management

ASI IT oversees the scanning process of all devices attached to a UASI network. A formal and updated inventory and monitoring log of all network scans 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.

Exceptions

Exceptions will be considered on a case-by-case basis. Exceptions must be reviewed and approved by the Institute Director and ASI Information Technology Administration.

History/Revision Dates

Effective Date	Version #	Author	Description
May 30, 2023	1.0	Nic Altamirano	Initial version.

Next Review Date: 5/30/2024