SPACE INSTITUTE
Information Technology

Shared Responsibility Model Policy

Effective Policy Date: May 30, 2023

Purpose of document: The document addresses the policy, procedures, and processes followed for the Arizona Space Institute regarding Shared Responsibility for Information Technology infrastructure and equipment within Arizona Space Institute (ASI) buildings.

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

Policy Statement

The ASI Information Technology (ASI IT) Shared Responsibility Model establishes clear guidelines for the division of Information Security and Compliance responsibilities between ASI IT and occupants of ASI facilities. This model ensures accountability and clarity in managing and securing IT devices within the ASI ecosystem. ASI IT is responsible for protecting the infrastructure that runs all of the services offered by ASI. This infrastructure is comprised of the hardware, software, networking, cloud providers, and facilities that run ASI services. Occupant responsibility will be determined by the ASI IT services that the occupant selects.

Policy Purpose

The ASI Shared Responsibility Model ensures effective and efficient management of IT resources, security, compliance, and support within the ASI. The shared responsibility model is necessary for:

1. **Clear Accountability:** A shared responsibility model defines the roles and responsibilities of different parties involved, clarifying who is accountable for various aspects of IT operations. This clarity avoids confusion and ensures that tasks and obligations are appropriately assigned and fulfilled.
2. **Optimal Resource Utilization:** By distributing responsibilities, a shared responsibility model allows for optimal utilization of resources. Each party can focus on their specialized areas of expertise, leading to increased efficiency and productivity. This prevents duplication of efforts and promotes a more streamlined approach to IT service management.
3. **Enhanced Security:** Information Security is a critical concern. In a Shared Responsibility Model, multiple stakeholders are accountable for implementing security measures. This collaborative approach helps to

address vulnerabilities, enforce security policies, and respond to incidents effectively. It ensures that everyone involved understands their role in maintaining a secure IT environment.

4. **User Empowerment:** In a Shared Responsibility Model, users are assigned specific responsibilities related to their use of IT equipment, services, and/or actions. This empowers users to take ownership and actively contribute to the overall IT ecosystem. It encourages adherence to IT policies, responsible usage of resources, and engagement in security practices. Users become more aware of their role in maintaining a reliable and secure IT infrastructure.
5. **Scalability and Flexibility:** A Shared Responsibility Model allows for scalability and flexibility in utilizing and managing IT operations. Responsibilities can be adjusted, allocated, or reassigned based on the evolving needs and resources of the ASI. This adaptability ensures that IT operations, security, and compliance can keep pace with organizational changes.
6. **Collaboration and Communication:** A Shared Responsibility Model fosters collaboration and communication among different stakeholders involved in IT management. It promotes dialogue, knowledge sharing, and coordination between IT departments, users, and other relevant parties. This collaborative environment enables effective problem-solving, innovation, and continuous improvement of IT services.

A Shared Responsibility Model provides a framework for efficient resource utilization, enhanced security, compliance, user empowerment, scalability, and collaboration. It ensures that all parties involved understand their roles and responsibilities while working together towards maintaining a robust and well-managed IT environment.

Who Needs to Know This Policy?

- All ASI users and building occupants that have/use a university purchased computer or device.
- All Arizona Space Institute users and building occupants that have/use a personal computer or device while on a University of Arizona Campus or accessing UArizona Resources. (Including but not limited to, users that are off-campus but accessing UA Resources via a Virtual Private Network – VPN).

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**
IT Equipment/Assets	IT Equipment/Assets refer to physical devices, components, and systems used in information technology (IT) environments to support various computing and communication functions. **IT Equipment/Assets can include a wide range of hardware devices and peripherals, such as:** - **Computers:** Desktops, laptops, servers, workstations, and thin clients that serve as the primary computing devices for users. - **Network Devices:** Routers, switches, modems, access points, and firewalls that facilitate network connectivity and data transfer. - **Storage Devices:** Hard disk drives (HDDs), solid-state drives (SSDs), network-attached storage (NAS), and storage area networks (SANs) used for data storage and retrieval. - **Peripherals:** Keyboards, mice, monitors, printers, scanners, projectors, and audio/video equipment that enhance user interactions and facilitate data input/output. - **Data Center Equipment:** Server racks, cooling systems, uninterruptible power supplies (UPS), backup generators, and cabling infrastructure that support the efficient operation of data centers. - **Communication Devices:** VoIP phones, mobile devices, video conferencing equipment, and telecommunication infrastructure required for effective communication and collaboration. - **Security Devices:** Surveillance cameras, access control systems, biometric scanners, and firewalls that protect IT assets and ensure data security.
ASI User	ASI Users refer to individuals who utilize a computer or device that is connected to a University of Arizona Space Institute (ASI) managed domain. These users have authorized access to the resources and services provided within the ASI domain. ASI, being a specialized institute dedicated to space-related research and education, extends its technological infrastructure to support its affiliated members, including students, faculty, researchers, and staff.
Building Occupant	Building Occupants refer to individuals who work or spend time within an ASI building, regardless of their role or affiliation. This broad category encompasses various individuals, including staff members, faculty, students, researchers, vendors, contractors, and other personnel associated with the University of Arizona Space Institute (ASI) or External Organizations working with UArizona.
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.
University Purchased Device	A University purchased device refers to any technology device that has been acquired using funds allocated by the Arizona Space Institute (ASI) of the University of Arizona. These devices are procured through official channels and are intended to support the academic, research, and administrative activities of ASI and its affiliated members.
Personal Device	A personal device refers to any technological device that has been acquired using an individual's personal funds or personal resources, rather than being purchased or provided by an organization or institution. These devices are typically owned and used by individuals for their personal needs, preferences, and convenience.

APPENDIX

The Key Principles of the Shared Responsibility Model

ASI IT Responsibilities:

ASI IT is responsible for UASI (University-owned and ASI-managed) devices. This includes devices provided by ASI and the network infrastructure supporting them.

A. **Network Infrastructure:**
    1. Design, implement, and maintain a secure and reliable network infrastructure within ASI facilities (Applied Research Building & Mission Integration Laboratory).
    2. Ensure network connectivity and bandwidth to meet the needs of users and occupants.
    3. Monitor network performance and address any issues or outages promptly.

B. **Power Infrastructure:**
    1. Maintain an efficient and uninterrupted power supply to ASI facilities, including backup power systems.
    2. ASI IT will work with the ASI Facilities team to ensure that they are conducting regular inspections and maintenance of power infrastructure to minimize the risk of outages and disruptions.

C. **Technical Support**
    1. Provide technical support to users and occupants within ASI facilities for university-owned and ASI-managed devices.
    2. Address hardware and software issues, troubleshoot problems, and ensure proper functioning of IT equipment.
    3. Offer assistance with software installations, updates, and patches.

D. **Security:**
    1. Implement and maintain robust security measures to protect ASI's network, systems, and data.
    2. Monitor security threats, vulnerabilities, and breaches, and take appropriate measures to mitigate risks.
    3. Enforce security policies and educate users about best practices for information security.

E. **Device Management:**
    1. Manage and maintain University-owned and ASI-managed devices within ASI facilities.
    2. Deploy necessary software and updates, configure settings, and ensure compliance with IT policies.
    3. Conduct regular inventory checks and asset tracking for efficient device management.

User Responsibilities for Non-ASI IT Assets:

ASI IT is not accountable for IT equipment, services, or devices that are not owned or managed by ASI.

Users that bring their own IT equipment into ASI facilities, including personal devices purchased with their own funds, are responsible and accountable for these devices which fall under the jurisdiction of their respective departmental IT. Users are required to work with their unit's IT department (e.g., Steward Observatory IT, Lunar and Planetary Laboratory IT, College of Engineering IT, etc.) to ensure the proper management, compliance, and maintenance of their non-ASI IT equipment.

Outlining these responsibilities ensures that users understand their obligations when bringing non-ASI IT equipment into ASI facilities and emphasizes the importance of collaboration with their respective unit's IT department for the proper management and resolution of any issues related to their devices.

A. Network Infrastructure:

1. Users must immediately report any network or connectivity issues related to their non-ASI IT devices to ASI IT. ASI IT can assist in contacting the home unit IT department for resolution.
2. ASI IT will offer general network connectivity for non-ASI IT devices. Users are responsible for configuring their devices appropriately to connect to the network and for ensuring compliance with network security protocols. ASI IT will assist with providing network segmentation for research instruments and workstations.

B. Power Infrastructure:

1. It is the responsibility of users to report any power-related issues, such as electrical outages or abnormalities, to ASI IT or the designated facility management personnel.
2. Users must not overload power outlets or use power-hungry devices that exceed the capacity of the electrical circuits.
3. Users must not tamper with or modify the power infrastructure within ASI facilities.
4. Users must not introduce any unauthorized or non-compliant power equipment or devices that may pose a risk to the power infrastructure or compromise its stability and reliability.

C. Technical Support:

1. ASI IT will provide general network connectivity and system support but is not responsible for troubleshooting or supporting non-ASI IT equipment brought by users. ASI IT will provide general guidance and support where possible, but for in-depth support, your unit's IT department would be the most suitable resource.

D. Security:

1. Users must comply with applicable IT policies, security practices, and software licensing requirements for their non-ASI IT devices.
2. Users must ensure that their non-ASI IT devices are protected against malware, viruses, and other security threats by installing and regularly updating appropriate security software. ASI IT does not take responsibility for patching or securing these devices.
3. It is the responsibility of the users to adhere to their unit's IT department's policies, guidelines, and procedures regarding the usage, access, and storage of data on their non-ASI IT devices.

E. Device Management:

1. Users are accountable for the physical maintenance and upkeep of their non-ASI IT equipment, including regular cleaning, hardware repairs, and replacement of faulty components.
2. It is the responsibility of users to keep their devices physically secure, including locking them when not in use and preventing unauthorized access to confidential information. 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.
3. Users must take appropriate security measures, such as setting up strong passwords, enabling device encryption, and utilizing antivirus software, to protect their devices and data from unauthorized access.

IT Asset Evaluation & Repurposing

The Arizona Space Institute (ASI) recognizes the importance of responsible resource management and aims to ensure the efficient and effective utilization of technology assets purchased using ASI funds. To achieve this, ASI has established a policy for the annual evaluation of these assets and a framework for their repurposing when they are no longer actively used by projects or groups.

If you're interested in learning more about this policy and how we handle the evaluation and repurposing of our IT assets, we encourage you to visit our website.

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

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