SPACE INSTITUTE
Information Technology

Mission Operation Center (MOC)
Shared Responsibility Model Policy

Effective Policy Date: August 30, 2023

Purpose of document: The purpose of this document is to establish clear guidelines and expectations for the shared responsibility of the Mission Operations Center (MOC) between the Arizona Space Institute (ASI) Information Technology (IT) Department and MOC personnel. This document outlines the roles and responsibilities of both parties in ensuring the effective operation, maintenance, and utilization of the MOC facilities and technical resources.

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

Policy Statement

The Arizona Space Institute (ASI) is committed to providing technical support for the Mission Operations Center (MOC) located at the Applied Research Building, Room 250. This policy outlines the shared responsibility between ASI IT and MOC personnel for the MOC and clarifies the roles and responsibilities of the ASI Information Technology (IT) Department and MOC personnel.

Who Needs to Know This Policy?

- To ensure the effective and secure operation of the Mission Operations Center (MOC), all Mission Personnel and ASI IT Personnel intending to utilize or support the MOC facilities are required to familiarize themselves with the ASI-006-MOC Shared Responsibility Policy and ASI-007-MOC Technology Standards. These policies and standards outline the technology standards, shared responsibility, and guidelines that govern the use of MOC resources and infrastructure.

Contacts

Responsible University Official: Director – Arizona Space Institute

Responsible University IT Official: Director, Information Technology – Arizona Space Institute

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

If there are questions on the policy, 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

Policy Compliance:

Non-compliance with this policy may result in restricted access to MOC facilities and technical resources. It is the responsibility of all individuals involved in MOC operations to adhere to this policy.

The Key Principles of the Shared Responsibility Model

ASI IT Responsibilities:

ASI IT is responsible for UASI (University-owned and ASI-managed) devices including but not limited to physical hardware (i.e., workstations, servers, storage arrays, etc.) and virtual hardware (i.e., virtual machines and VM resources). This includes devices provided by ASI and the network infrastructure supporting them.

a. **Technical Support:** ASI IT will provide technical support for the Network, Audio-Visual (AV) systems, and shared spaces within the MOC. This support includes but is not limited to network connectivity, AV equipment setup and maintenance, and ensuring the proper functioning of shared spaces.

b. **Infrastructure Utilization:** ASI IT maintains a VMware Infrastructure that will be utilized to provide the technical resources required by the MOC, depending on the specific mission requirements. Resources within this infrastructure will be made available for MOC personnel to access and utilize during their mission-related activities.

c. **Maintenance and Upkeep:** ASI IT will be responsible for regular maintenance and upkeep of the MOC's technical infrastructure. This includes performing updates, security patches, and ensuring the reliability of the systems.

Mission Operations Center (MOC) Responsibility:

a. **Mission-Specific Requirements:** MOC personnel are responsible for communicating mission-specific technical requirements to ASI IT in a timely manner. This includes any specialized software, hardware, or network configurations needed for mission success.
ASI IT's Service Agreement:
https://it.space.arizona.edu/compliance/service-agreement

b. **Equipment and Space Usage:** MOC personnel are responsible for the proper use and care of all equipment and shared spaces within the MOC. This includes reporting any issues or malfunctions promptly to ASI IT.

c. **Security and Access Control:** MOC personnel must adhere to all security protocols and access control measures established by ASI Facilities to safeguard the technical resources and data within the MOC.

d. **Training:** MOC personnel will receive training as needed to operate the technical equipment and systems within the MOC effectively. Training requirements and schedules will be coordinated between ASI IT and MOC Personnel.

Additionally, all MOC personnel will need to complete annual information security awareness training provided by the University of Arizona Information Security Office in order to retain network access.

Policy Review:

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. Any proposed changes will be communicated to all relevant parties.

Approval:

This policy has been approved by the ASI Director and is effective as of the date specified above.

Exceptions

Exceptions regarding technical responsibilities 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
August 30, 2023	1.0	Nic Altamirano	Initial version.

Next Review Date: 5/30/2024