SPACE INSTITUTE
Information Technology

Mission Operation Center (MOC)

Technology Standard

Effective Standard Date: August 30, 2023

Purpose of document: This document serves to establish and communicate the comprehensive technology standards governing the utilization of the Mission Operations Center (MOC) located within the Applied Research Building. The primary objective of this document is to provide a detailed framework that outlines the technical capabilities, security controls, compliance requirements, and backup procedures associated with the operation of the MOC.

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

Who Needs to Know This Standard?

- This standard applies to all ASI IT Department staff and MOC personnel involved in the operation and utilization of the MOC facilities.

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 Standard

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

Definitions

Term	Definition as it relates to this standard
ASI IT Personnel	Staff hired by the Arizona Space Institute Information Technology Department.
Mission Personnel	Mission personnel refers to individuals who are directly involved in the planning, execution, and support of a specific mission, project, or operation.
Mission Team	Mission team refers to a group of individuals who collaborate and work together to achieve specific goals or objectives related to a particular mission, project, or task.

Virtual Machine	A "virtual machine" (VM) is a software-based emulation of a physical computer. It acts as a self-contained operating environment that runs on a physical computer, known as the host machine, but behaves like a separate and independent computer system.
Controlled Unclassified Information (CUI)	Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.
International Traffic in Arms Regulations (ITAR)	A United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives.
Export Administration Regulations (EAR)	A set of United States export guidelines and prohibitions. They are administered by the Bureau of Industry and Security and regulates export and export restrictions.

APPENDIX

Explanation of Technical Resource Provisioning:

Arizona Space Institute Information Technology (ASI IT) is committed to providing the technical resources necessary for missions conducted within our ecosystem. Our data center infrastructure has been meticulously designed for scalability, but it's important to note that we operate with limited resources. To ensure the most efficient and effective support for the mission, a consultation with ASI IT is a crucial initial step.

During the consultation, ASI IT will collaborate closely with the mission team to determine the specific equipment and resources required. Our goal is to ensure that the resources requested align with the capabilities of our infrastructure. If it is determined that our resources can support the mission's requirements, ASI IT will proceed with providing the necessary virtual hardware.

Virtual Hardware Provisioning:

ASI IT will take responsibility for setting up the required virtual machines with the operating system(s) specified by the mission team. However, it is important to note that day-to-day operations and configurations of these virtual machines will be the responsibility of the mission team. This approach allows for flexibility and customization, putting control in the hands of those who best understand the mission's unique demands.

In terms of security, ASI IT will ensure that all virtual machines are equipped with the necessary security controls to protect against potential threats.

Cost Determination and Resource Allocation:

The costs associated with using the Mission Operations Center (MOC) and utilizing Arizona Space Institute (ASI) IT resources will be assessed on a project-specific basis. ASI recognizes that each project may have unique requirements and resource needs. Therefore, the determination of costs will be made by ASI leadership, taking into account the scope and technical demands of the project.

Point of Contact for MOC Inquiries:

For any inquiries related to the use of the Mission Operations Center, individuals and teams are encouraged to engage directly with the ASI Director. The ASI Director will serve as the primary point of contact for discussions and questions regarding MOC utilization.

Hardware Requirements for Specific Missions:

In cases where a mission requires equipment or resources that are not currently within ASI's existing inventory, a detailed hardware requirements assessment will be conducted during the initial consultation between ASI IT and Mission Operations Personnel. The cost associated with procuring additional hardware needed for the mission will be the responsibility of the mission requiring such hardware.

Expansion of Existing Hardware:

In certain instances, expanding the capabilities of the existing hardware infrastructure may be a viable option to meet mission requirements. This expansion could involve activities such as purchasing additional storage for the storage array or adding an extra node to the virtual machine (VM) environment. Any hardware acquired to expand the existing environment will become the property of ASI IT. This is because removing or decommissioning such hardware could disrupt ongoing MOC operations.

Security Controls for Virtual Machines:

To ensure the highest level of security and compliance, all virtual machines provided by ASI IT will be configured with robust security controls that adhere to best practices. These controls encompass various aspects of security, including but not limited to:

1. **Account Permissions:** User access to virtual machines will be carefully controlled and aligned with the university information security office governance to prevent unauthorized access and ensure data protection.
2. **Authentication Methods:** Secure authentication methods will be implemented to verify the identity of users accessing virtual machines, enhancing overall system security.
3. **Encryption Policies:** Data encryption policies will be enforced to safeguard data in transit and at rest, protecting sensitive information from potential threats.

Mission personnel must consult with ASI IT in the event of any issues that may hinder their ability to perform their duties effectively. ASI IT will provide support, troubleshoot technical problems, and address any concerns related to the virtual machines provided.

Restrictions on Changes:

It is essential to note that changes to the configuration or settings of these virtual machines will only be made by ASI IT personnel. This restriction is in place to maintain the integrity and security of the virtual machine environment. Unauthorized modifications can pose security risks and disrupt mission operations.

Backup Procedures:

To safeguard mission-critical data and operations, backup procedures are required by the mission team and will be discussed in detail during the initial consultation with the ASI IT team. This discussion will cover the frequency and methods of data backup, as well as data recovery processes in the event of unforeseen issues.

ASI IT places a high priority on data integrity and availability, and we are committed to working collaboratively with the mission team to ensure that the technical requirements are met while maintaining the highest standards of security and reliability. Our aim is to support your mission's success by providing the necessary technical resources and expertise.

Compliance and Hosting Considerations:

At the Arizona Space Institute (ASI), we take compliance and security matters seriously to ensure the utmost protection of sensitive information and mission-critical data. Depending on the specific compliance requirements of the mission, ASI will carefully assess and communicate our capabilities to host your mission.

Attention: As of **August 2023**, ASI is unable to provide resources for projects that involve Controlled Unclassified Information (CUI) or NIST SP 800-171 compliance. We are committed to maintaining a secure and compliant environment, and our policies reflect this commitment. ASI does not currently have this capability, but we are actively working towards achieving it.

NIST 800-171 Compliance Efforts:

ASI acknowledges the importance of compliance with the National Institute of Standards and Technology (NIST) Special Publication 800-171 (NIST 800-171) guidelines, which are designed to enhance the security of Controlled Unclassified Information (CUI). While we are actively working towards achieving compliance with NIST 800-171, it is essential to note that as of the current date, we cannot fully meet all the prescribed objectives at this time.

We appreciate the understanding and cooperation as we prioritize the security and compliance of our mission operations. If you have any specific questions or require further information regarding compliance and hosting considerations, please do not hesitate to reach out to our ASI IT team for clarification and guidance. Your mission's success and security are of paramount importance to us.

Handling of Export Control Information (ECI):

For all projects or missions that involve Export Control Information (ECI), it is imperative to adhere to rigorous compliance standards. ASI places a high priority on maintaining the security and integrity of ECI. Therefore, the following procedures and responsibilities must be followed:

University of Arizona Export Control Office (ECO): All projects or missions dealing with ECI must collaborate with the University of Arizona Export Control Office. The ECO is the designated authority for managing and overseeing ECI matters. Their expertise and guidance are essential to ensure compliance with export control regulations. This includes projects and missions that have CUI, ITAR, and EAR. MOC project personnel are

required to follow the procedures and protocols put in place by the ECO such as a Technology Control Plan. **Contact**: export@arizona.edu

ASI IT Consultation: ASI IT is available to consult and assist in determining the technology requirements for projects involving ECI. We can help assess the technical aspects of the project, including infrastructure and resource needs. However, ASI IT cannot provide guidance or information related to Controlled Unclassified Information (CUI), International Traffic in Arms Regulations (ITAR), or Export Administration Regulations (EAR).

Security and Compliance: The Arizona Space Institute Information Technology Department (ASI IT) employs a comprehensive array of tools and methods to safeguard security and ensure compliance within our technology infrastructure. These measures include, but are not limited to:

a. **University of Arizona Logging and Monitoring Program:** We utilize the University of Arizona's Logging and Monitoring Program to continuously monitor and analyze system logs and network traffic for signs of security threats or anomalies. This proactive approach helps us identify and respond swiftly to potential security issues.
b. **Network Scanning:** Regular network scanning procedures are implemented to assess the security posture of our systems. These scans help us identify vulnerabilities and weaknesses, enabling us to apply necessary security patches and updates promptly.
c. **Sophos Malware and Antivirus:** ASI IT employs Sophos, a robust malware and antivirus solution, to protect against a wide range of malicious software threats. This software detects, quarantines, and removes malware to maintain the integrity of our systems.
d. **Encryption at Rest and in Transit:** Data security is paramount. We implement encryption both at rest and in transit to ensure that sensitive information remains confidential and protected from unauthorized access. This approach safeguards data whether it's stored on our systems or transmitted over networks.

Standard Compliance:

Non-compliance with this standard 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 standard.

Standard Review:

This standard 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 standard 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