Sam Mendez

Lab #5

Policy Header:

Policy Name: King Sam Space Station Identity and Access Management (IAM) Policy

Version: 1.0

Approval Date: 2/8/24

Effective Date: 2/11/24

Policy Objectives:

Purpose:

The purpose of this IAM Policy is to establish guidelines, principles, and best practices for managing identities and controlling access within King Sam Space Station. This policy aims to safeguard sensitive information, ensure compliance with interstellar standards, and mitigate risks associated with unauthorized access in the lunar environment.

Scope:

This policy applies to all astronauts, mission control personnel, contractors, and any entity with access to King Sam Space Station's information systems and data.

Responsibilities:

The Space Station Operations department is responsible for the implementation, maintenance, and enforcement of this IAM policy. All space station inhabitants are responsible for adhering to the guidelines outlined in this policy.

Policy Content:

User Identification:

All astronauts and personnel must be uniquely identified within the space station's system.

User identification will follow the principles outlined in ISO/IEC 27001:2013 and NIST SP 800-63, adapted for the lunar environment.

Authentication:

Biometric authentication and smart card access are mandatory for accessing sensitive areas and data.

Lunar Environment Suit (LES) authentication protocols will adhere to the complexity requirements specified in NIST SP 800-63.

Regular LES password changes are enforced, and password reuse is prohibited.

Authorization:

Access privileges are assigned based on the principle of least privilege (PoLP) to house various tasks in the lunar environment.

Lunar Role-based access control (LRBAC) is implemented to manage user permissions.

Access reviews are conducted periodically to ensure continued appropriateness of access levels in the unique space environment.

Auditing:

All access and authentication events are logged and regularly reviewed.

Audit logs will be maintained to comply with interstellar security standards.

Suspicious or unauthorized activities must be reported promptly to the Space Station Security team.

Policy Enforcement and Penalties:

Violations of this IAM policy may result in disciplinary action, including but not limited to verbal or written warnings, suspension of space station access privileges, or return to Earth, depending on the severity of the violation. Legal action may be pursued if necessary, following interstellar laws.

Review and Update Procedures:

This IAM policy will be reviewed annually or as needed to adapt to changes in space station operations, technology, or interstellar regulations.

Updates will be communicated to all relevant space station inhabitants, and training will be provided to ensure awareness of policy changes.

Key Standards:

ISO/IEC 27001:2013

NIST SP 800-63

OpenID Connect (Adapted for lunar environment)

SAML 2.0 (Adapted for lunar environment)

OAuth 2.0 (Adapted for lunar environment)

References:

"Identity and Access Management: An Introduction" - ISC2

NIST Special Publication 800-63

ISO/IEC 27001:2013 Official Documentation

OpenID, SAML, OAuth Documentation

What are the key components of an IAM policy?

User Identification, Authentication, Authorization, Auditing, Policy Enforcement and Penalties, Review and Update Procedures.

Name at least two standards that ca be referenced for IAM policy development.

ISO/IEC 27001:2013: An international standard specifying the requirements for establishing, implementing, maintaining, and continually improving an information security management system.

NIST SP 800-63: Guidelines from the National Institute of Standards and Technology providing technical requirements for digital identity management, particularly focused on authentication.

What is the Difference between Authentication and Authorization?

Authentication: Verifying the identity of users or systems, ensuring they are who they claim to be. In the context of King Sam Space Station, this involves methods like biometric authentication, smart cards, or lunar environment suit protocols.

Authorization: Determining and granting access permissions based on authenticated identities. It dictates what actions or resources a user is allowed to access, considering roles and responsibilities in the lunar environment.

Why Auditing is Essential in IAM?

Auditing is crucial in IAM for several reasons. It provides a detailed record of who has accessed what information and when. It helps in detecting and investigating security incidents or unauthorized access. IAM also supports compliance efforts by demonstrating adherence to security policies and standards. Lastly, it aids in identifying areas for improvement in the IAM processes.

What are the potential penalties for not adhering to an IAM policy?

Penalties for non-compliance may include:

* Verbal or written warnings.
* Suspension of space station access privileges.
* Return to Earth, depending on the severity of the violation.
* Legal action in accordance with interstellar laws.

These penalties are essential for enforcing the IAM policy, maintaining security, and ensuring the well-being of King Sam Space Station and its inhabitants.

Top of Form