Sam Mendez

Lab 7

Security Operations Policy Development Lab

**King Sam Lunar Space Station Policies**

**Incident Response Policy**

**Purpose**

The purpose of this Incident Response Policy is to establish a structured and coordinated approach to detecting, responding to, and mitigating security incidents within the King Sam Lunar Space Station.

**Scope**

This policy applies to all personnel, systems, and assets within the King Sam Lunar Space Station.

**Policy**

The King Sam Lunar Space Station will maintain an incident response capability to identify, manage, and recover from security incidents promptly and effectively.

**Roles and Responsibilities**

Incident Response Team (IRT): Responsible for managing and responding to security incidents.

System Administrators: Report and assist in incident response efforts.

Security Officers: Oversee incident response activities and coordinate with external entities.

**Incident Classification**

Incidents will be classified based on severity, impact, and nature, following the guidelines outlined in NIST SP 800-61 and ISO/IEC 27035.

**Incident Reporting**

All personnel must promptly report any suspected security incidents to the Incident Response Team.

**Incident Response Procedures**

Identification: Quickly identify and verify the incident.

Containment: Isolate affected systems to prevent further damage.

Eradication: Remove the root cause of the incident.

Recovery: Restore affected systems to normal operations.

Lessons Learned: Conduct a post-incident review to improve future response.

**Review and Audit**

Regular reviews and audits of incident response activities will be conducted to ensure effectiveness and compliance with NIST SP 800-61 and ISO/IEC 27035.

**Key Standards**

[NIST SP 800-61](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

[ISO/IEC 27035](https://www.iso.org/standard/44379.html)

**References**

[NIST SP 800-61](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

[ISO/IEC 27035](https://www.iso.org/standard/44379.html)

**Disaster Recovery Policy**

**Purpose**

The purpose of this Disaster Recovery Policy is to establish guidelines and procedures to ensure the prompt and effective recovery of critical systems and data following a disruptive incident.

**Scope**

This policy applies to all critical systems and data within the King Sam Lunar Space Station.

**Policy**

The King Sam Lunar Space Station will implement a comprehensive disaster recovery program to minimize the impact of disruptions and ensure the continuity of operations.

**Roles and Responsibilities**

Disaster Recovery Team: Responsible for developing, implementing, and maintaining the disaster recovery plan.

System Owners: Identify critical systems and data for inclusion in the plan.

IT Department: Implement and maintain technical aspects of the disaster recovery plan.

**Recovery Strategies**

Define strategies for data backup, system redundancy, and alternative processing facilities following NIST SP 800-34 and ISO/IEC 27031.

**Implementation Steps**

Risk Assessment: Identify potential threats and vulnerabilities.

Plan Development: Create a detailed disaster recovery plan.

Implementation: Execute the plan as needed during a disaster.

Testing and Revision: Regularly test and update the plan to ensure effectiveness.

**Testing and Maintenance**

Conduct regular tests and exercises of the disaster recovery plan to ensure its functionality and relevancy.

**Key Standards**

[NIST SP 800-34](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final)

[ISO/IEC 27031](https://www.iso.org/standard/44374.html)

**References**

[NIST SP 800-34](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final)

[ISO/IEC 27031](https://www.iso.org/standard/44374.html)

**Business Continuity Policy**

**Purpose**

The purpose of this Business Continuity Policy is to ensure the King Sam Lunar Space Station's ability to continue critical operations in the face of disruptions.

**Scope**

This policy applies to all critical business functions and processes within the King Sam Lunar Space Station.

**Policy**

The King Sam Lunar Space Station will establish and maintain a business continuity program to safeguard against potential disruptions and ensure the ongoing delivery of critical services.

**Roles and Responsibilities**

Business Continuity Team: Develop and maintain the business continuity plan.

Department Heads: Identify critical functions and resources within their departments.

Employees: Cooperate with business continuity efforts and participate in training.

**Business Impact Analysis**

Conduct a Business Impact Analysis (BIA) to identify critical functions, resources, and recovery time objectives (RTOs).

**Continuity Strategies**

Define strategies for maintaining critical operations during disruptions based on the outcomes of the BIA. Align strategies with NIST SP 800-34 and ISO 22301.

**Training and Awareness**

Provide ongoing training and awareness programs to ensure all personnel are familiar with business continuity procedures.

**Key Standards**

[NIST SP 800-34](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final)

[ISO 22301](https://www.iso.org/standard/75106.html)

**References**

[NIST SP 800-34](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final)

[ISO 22301](https://www.iso.org/standard/75106.html)

**Questions:**

1. What are the key differences between an Incident Response Policy and a Disaster Recovery Policy?

Incident Response Policy focuses on immediate response to security incidents aiming to minimize damage, contain threats and restore normal operations. Disaster Recovery Policy concentrates on recovering critical systems after disaster has happened.

2. How does a Business Impact Analysis (BIA) contribute to Business Continuity Planning (BCP)?

BIA contributes to BCP by identifying and prioritizing critical business functions, resources and processes. BIA establishes Recovery Time Objectives and identifies dependencies between different functions. The information gathered by BIA helps guide the development of strategies for continuity ensuring that resources are allocated appropriately to minimize downtime and loss.

3. What are the key roles of an Incident Response Team?

The key roles of an Incident Response Team are the incident commander, investigator/analyst, technical support, communication coordinator, compliance representative and public relations liaison

4. Why is it important to regularly test and update your Disaster Recovery Plan?

It is important to regularly test and update you DRP to ensure that the plan remains effective in the current environment. Technology and systems change, testing helps identify weaknesses and gaps in the plan, allowing for improvements.

5. What are the key elements to consider when developing a Business Continuity Policy?

The key elements to consider when developing a BCP is identifying critical functions, assess risks, and set priorities. By defining roles, conducting regular testing, and maintaining documentation greatly helps in the development of an effective BCP.