**U07A1 – Operational Management Policy**

**Chris Misch**

School of Business, Technology, and Health Care Administration, Capella University

IT4076: Security Management and Policies

Stuart McCubbrey

May 2023

1. **Overview**

Operational security management is the process that prevents sensitive information from being exposed to unauthorized entities. Creating proper procedures for the managing of organizational structures is vital for buisness continuity, viability, and integrity.

* 1. **Purpose**

The purpose of this policy is to layout the groundwork for creating policies that will protect the confidentiality, integrity, and availability of systems and resources of the organization. The policies created will cover identifying, protecting, detecting, responding, and recovering protected systems, data, and resources to ensure the survivability and growth of the organization.

* 1. **Scope**

This policy covers information asset types defined in the NIST SP800-160v1r1. The policies written here will apply to all employees, contractors, vendors, volunteers, and all others who use this organization’s systems or resources.

1. **Policy**

This policy will be reviewed once a year to ensure it remains current. At the time of review changes or updates may be implemented and a change log will be created and updated for any new changes to this policy.

* 1. **Contingency Planning (CP)**

Contingency planning will outline the developing strategies and procedures that address potential disruptions to normal business operations. This includes identifying critical systems and resources, implementing backup and recovery mechanisms, and establishing incident response plans. The main goal is to restore normal operations of the hospital with minimal cost and disruption after a manmade or natural disaster.

The hospital’s contingency plan will adhere to the NIST SP800-34r.1 guidelines which provide a comprehensive framework for contingency planning for federal information systems. The plan will guide the organization when a disaster occurs, ensuring limited buisness disruption by following these seven steps:

1. Policy statement: A formal policy that outlines the organization’s commitment to contingency planning.
2. Business impact analysis (BIA): An assessment of the potential impact of disruptions on the organization’s critical functions, processes, and resources.
3. Identification of preventative controls: Identification and implementation of measures to mitigate risks and prevent disruptions.
4. Contingency strategies: Development of strategies and approaches to respond to different types of disruptions, including backup and recovery mechanisms.
5. Contingency plan: Documenting the detailed actions and procedures to be followed during and after a disruption, including roles and responsibilities.
6. Training and testing: Regular training of personnel involved in contingency planning and conducting exercises to test the effectiveness of the plan.
7. Regular updates: Ongoing review and updates of the contingency plan to reflect changes in technology, processes, and organizational needs.

To develop a CP effectively a management team must be created that involves the Chief Information Officer (CIO), Chief Information Security Officer (CISO), key IT and business managers, along with a system administrator. The team will follow NIST guide for contingency planning ensuring the plan is comprehensive, aligned with best practices, and capable of minimizing business disruptions in the event of a disaster.

* 1. **Vital Records Management**

Vital records management is crucial to the overall organizational security and continuity of the hospital system. It includes monitoring, logging, and maintenance of records in compliance with regulations and rules set by local, reginal, and global governments. Securing vital records effectively is crucial for the hospital to remain competitive and compliant with all relevant regulations.

Types of vital records will include patient information, records management, legal papers, compliance, operations, risk management, IT records, and any collection of documents that fall under local rules and regulations.

To ensure the confidentiality, integrity, and availability (C-I-A) of all records is achieved proper controls must be created. These controls can be in the form of group policies and access controls that limit users and groups from accessing information beyond their authorized scope (such as need-to-know authority or scope of practice). Compliance with relevant regulations, such as HIPAA §164.308(a)(3)(ii)(B), is crucial in establishing these controls.

When managing vital records, they should be inventoried, secured, and easy to recover in accordance with the hospital’s Business Continuity Plan and Disaster Recovery plan. Proper records management is crucial in preparing, managing, and recovering from disasters or disruptions to the hospital system. In the event of a disaster vital records must be accessible to ensure the continuity of business to maintain the health and safety of all employees, patients and entities directly or indirectly associated with the hospital.

* 1. **Physical Safeguards**

Physical safeguards will focus on security of the organization’s physical assets, such as equipment, data centers, and facilities. Measures will be implemented to control access, monitor, and record activities and protect against unauthorized intrusion or damage.

Physical safeguards are important in assuring physical policies, measures, and procedures are in place to protect the organization from physical hazards. All physical aspects of the organization must be considered when protecting sensitive information and data in the hospital. Access controls must be implemented to control the flow of physical movement that could gain access to sensitive systems and data. There will be contingencies created in the case of sensitive information being exposed that minimize the loss of data while restoring normal operational procedures.

Records must be kept and stored securely regarding all access to the hospital facility. This will include physical entry into different areas of the hospital along with any logical controls that restrict physical access. Records will also include any maintenance, creation, deletion, or change in physical controls.

* 1. **Technical Safeguards**

Technical safeguards will address the protection of information systems and networks. This includes implementing security controls such as firewalls, intrusion detections systems, encryption, access controls, and regular patch management.

Access controls ensure technical aspects of the hospital are secure. These controls involve the form of unique usernames and passwords as well as establishing emergency access procedures in the event of a breach of authority. In addition to this controls can be implemented that add encryption to data in transit and data at rest to reduce the risk of unauthorized access.

Adding technical safeguards will ensure that the hospital system and network are secure from unauthorized access. This is crucial in ensuring data integrity and confidentiality for patient health information (PHI) and patient personally identifiable information (PII), and organization trade secrets. By utilizing risk analysis and risk management to assess the vulnerabilities, the hospital can enhance the security of its network, protecting both external and internal threats.

1. **Policy Compliance**

All employees, contractors, vendors, and volunteers must comply with this Operational Management Security Policy, Failure to follow this policy will result in disciplinary action, up to and including termination of employment, services, or contracts.

1. **Roles and Responsibilities**

Roles and Responsibilities are assigned to current positions within High Class Healthcare.

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| CEO | Oversee and authorize final approval of any changes made to this policy.  Provide leadership and guidance to team members and other stakeholders.  Ensure the development, implementation, and maintenance of the policy. |
| CIO | Coordinate security initiatives and activities.  Stay up to date with emerging threats and vulnerabilities and recommend counter measures as necessary.  Coordinate security initiatives and activities. |
| Network Administrator | will ensure information security policies are known and understood within their respective departments.  Keep up to date with emerging threats and vulnerabilities and recommend counter measures as necessary.  Conduct regular assessments, audits, and testing |
| IT Administrator | Ensure proper configuration, patching, and updating of systems.  Provide training and awareness.  Implement and maintain technical security measures |
| Help Desk Supervisor | Assist in incident response when needed.  Assist IT Administrator where needed. |

1. **Related Standards, Policies, and Processes**

NIST SP800-160v1r1

HIPAA Security Rule 45 CFR §164.308(a)(3)(ii)(B).

HIPAA Security Series

NIST SP800-53A

1. **Definitions and Terms**

CEO – Chief Executive Officer

CIO – Chief Information Officer

C-I-A – Confidential, Integrity, and availability. Refers to ensuring sensitive information is safe, secure, and available to authorized entities only.

NIST – National Institute of Standards and Technology

HIPAA -Health Insurance Portability and Accountability Act

1. **Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Summary of Changes | Approval |
| 1.0 | 05/20/2023 | Creation of new policy | Mark Moneybags, CEO |