**U06A1 – Physical and Environmental Security Policy**

**Chris Misch**

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

IT4076: Security Management and Policies

Stuart McCubbrey

May 2023

1. **Overview**

Protecting the physical and environmental aspects of the hospital is vital to ensuring the safety and well-being of sensitive information, people, and equipment. Protecting the physical and environmental aspects of the hospital will result in the compliance of assuring confidentiality, integrity, and availability of all systems and functions of the hospital.

* 1. **Purpose**

This policy will protect the Hospital system resources, resource system housing, and the facilities used to support their operation. Threat to physical and environmental security can range from natural disaster to human error. This policy will eliminate or reduce the threat against the secure operation of the hospital network, systems, and stored data.

* 1. **Scope**

This policy will cover all physical areas of the hospital including property perimeter, parking lot, outer shell and inner shell of the building, and all physical items and areas within the hospital walls. This policy applies to all entities, employees, volunteers, contractors, vendors, visitors, patients, and anyone that enters or uses the Healthcare property.

1. **Policy**

Physical property risk can be from by both natural and man-made disaster. Natural disaster can include fire, flood, tornados, earthquakes, hurricanes, and anything else not otherwise controlled by man and technology.

Man-made disasters can be from break-ins, theft, fire, flood, loss of system integrity, unauthorized disclosure of information, and physical damage to systems, devices, data, storage media and any other technology that is used within and outside the hospital.

* 1. **Physical Access Controls**
     1. The security perimeter should have a staffed reception area to control access to the main entry of the hospital and appropriate security controls for secondary entrances. HIPAA: 164.310(a)(1)(ii), ISO: 9.1.1, NIST: S800-12(15.1), NFPA: 101 2012ed.
     2. Secondary entrances will be locked from the outside but may remain unlocked according to local and reginal fire safety laws and regulations. NIST: SP800-12(15.1), NFPA: 101 2012ed, OSHA 1910
     3. Each area of the hospital will be sectioned off according to security sensitivity. Extra security controls will be increased as needed to provide adequate protection. HIPAA: 164.310(a)(1), ISO: 9.1.1, NIST: SP800-12(15.1)
     4. Security cameras should monitor all doorways into, out of, and throughout the facility 24 hours a day. NIST: SP800-12(15.1), PCI: 9.1.1
     5. Logs shall be maintained for all authorized and unauthorized physical access.
     6. Physical access to utilities such as gas, electricity, phone lines, internet connection, water, and any other elements required for system’s operations will be identified and access to them will be controlled. NIST: SP800-12(15.1)
  2. **Physical Entry Controls**
     1. Identification badges must be worn by all entities that enter the facility. They must always be visible. Temporary badges must include an expiration. All badges will include the wearer’s identity (full name and picture), position, title, and level of authorization.
     2. Sensitive areas of the facility must be secured so that only the authorized individuals may access the areas. HIPAA: 164.310(a)(1), NIST: SP800-12(15.1)
     3. Security personnel located at each reception area, employees, and volunteers will be responsible for ensuring all entities withing the facility are wearing their badges. PCI: 9.3
     4. Any lost or stolen badges must be reported to the security office immediately.
  3. **Natural Disaster Controls**
     1. All doorways and windows designated as emergency exits will be clearly identified and unlocked according to local and reginal fire safety laws and regulations. NFPA: 101 2012ed.
     2. Fire detection and suppression systems should be in place. Suppression systems will have an adequate supply of water available to them. Where fire suppression systems are not adequate the use of fire extinguishers will be used. All staff must be trained in the proper usage of this device. OSHA: 1910.157, NIST: SP800-12(15.2)
     3. Portable fire extinguishers must be approved by OSHA and will be distributed, maintained, inspected, and tested according to OSHA rules. OSHA: 1910.157
     4. There must be a contingency plan created in case of an emergency due to natural or human made disasters. §164.310(a)(2)(i)
     5. There should be power generators available in case of power outage. §64.310(a)(2)(i)
     6. All combustible material must be stored securely and away from combustible materials according to local and reginal safety rules. OSHA: 1910 Subpart H
  4. **Information Technology Storage Rooms** 
     1. Information technology rooms that support the main network will be locked and use multilayered access controls. §164.310(a)(1)
     2. Proper ventilation in closed IT closets and rooms must be used. OSHA: 1910.94(a)(4), OSHA: 1910.176
     3. Access to technology rooms must be reviewed quarterly and revoked immediately when it is no longer needed. HIPAA: 164.310(a)(1)(iii)
     4. Walls (including sidewalls, floors, and ceiling) surrounding Information Technology rooms must be non-combustible and resistant to fire. All opening to these walls must be self-closing and resistant to fire.

1. **Policy Compliance**

Failure to comply with this policy may result in legal and federal prosecution and up to and including termination.

If a failure to comply with this policy is found it must be reported to the appropriate department and follow proper incident response procedures set forth in the Incident Response Policy.

1. **Roles and Responsibilities**

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| Facilities Manger | will ensure that the perimeter of the facility is secure and access to the hospital is properly maintained. |
| Supervisors and managers | will ensure information security policies are known and understood within their respective departments |
| Employees located at reception area | responsible for creating and distributing badges to visitors, vendors, and anyone without a badge |
| All employees | will ensure all entities in the facility wear the appropriate ID badge. If someone is not wearing a badge it must be reported to reception and security department right away. |
| IT security department and Human Resources | Perform auditing of access control measures and policy compliance |

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

NIST SP800-12

NFPA 101 & 99, 2012 Edition

PCI

OSHA 1910

Code of Federal Regulations Title 45 Part 164 Subpart A (§164)

Incident Response Policy

1. **Definitions and Terms**

OSHA 1910 – Occupational Safety and Health Standards is the regulatory agency of the US Department of Labor

NFPA – Nation Fire Protection Association is a global non-profit agency devoted to eliminating death, injury, property and economic loss due to fire, electrical and related hazards.

PCI – Payment Card Industry is an information security standard used to handle credit cards and payment services.

Entities – Can include employees, vendors, contractors, service animals, etc.

1. **Revision History**

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

1. **Resources**

*Codes and standards | NFPA*. (n.d.). <https://www.nfpa.org/Codes-and-Standards>

*NIST SP 800-12: Chapter 15 - Physical and Environmental Security*. (n.d.). https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter15.html