Cybersecurity Policy for Low-Risk Healthcare Environments

Version: 1.0

Effective Date: [Date]

Approved By: [Your Name/Designation, e.g., CISO]

1. Introduction

This Cybersecurity Policy outlines the minimum security requirements for [Organization Na
order to protect the confidentiality, integrity, and availability of patient data and other
sensitive information. This policy is designed specifically for low-risk environments within th
healthcare organization, characterized by limited direct patient care activities, minimal ePH
(electronic Protected Health Information) storage, and restricted network connectivity to cr
systems. This policy is aligned with the principles of ISO/IEC 27001 and aims to establish a
foundational cybersecurity posture that minimizes risks and promotes a security-conscious
This policy applies to all employees, contractors, vendors, and other individuals who access
[Organization Name]'s information systems and data, regardless of location. Failure to com
this policy may result in disciplinary action, up to and including termination of employment
contract.

2. Risk Assessment

Given the low-risk environment, a simplified risk assessment process will be implemented a
reviewed annually. The assessment will focus on identifying and prioritizing potential threat
vulnerabilities related to the organization's specific operations.

* **Frequency:** Annually, or more frequently if significant changes occur to the environm
(e.g., new systems, processes, or regulations).
* **Scope:** Limited to systems and data within the defined low-risk environment.
* **Methodology:** A qualitative risk assessment approach will be used, focusing on likeli
impact. Common threats considered will include phishing attacks, malware infections, unau
access to data, and loss or theft of devices.
* **Documentation:** A Risk Register will be maintained, documenting identified risks, as

likelihood and impact, and implemented mitigation strategies.

*   **Mitigation:** For identified risks, appropriate mitigation strategies will be implemente based on the "Risk-based thinking" principle of ISO 27001. These may include technical cor administrative procedures, and physical security measures.

3. Data Protection

Even in a low-risk environment, protecting data is paramount. This section outlines the data protection requirements:

*   **Data Classification:** Data will be classified based on sensitivity (e.g., Confidential, Internal Use Only, Public). While ePHI storage is limited, any identified ePHI will be classifie as Confidential.

*   **Data Encryption:** Encryption of data at rest is not mandatory for systems within this risk environment, but encryption of portable storage devices (e.g., USB drives) is required i contain any sensitive data. Encryption of data in transit (e.g., via HTTPS) is required for web based applications.

*   **Data Backup:** Regular backups of critical data will be performed to ensure business continuity and data recovery in case of system failures or data loss. Backup frequency and policies will be defined based on the Recovery Time Objective (RTO) and Recovery Point Ob (RPO) for each system. Backups must be stored in a secure location, physically separated f primary data.

*   **Data Disposal:** Data must be securely disposed of when no longer needed. This inclu wiping or physically destroying storage media. Deletion alone is not sufficient.

*   **Data Loss Prevention (DLP):** DLP tools are not required, but users should be trained t accidentally or intentionally sharing sensitive data through unsecured channels.

4. Access Controls

Access to systems and data within the low-risk environment will be managed based on the least privilege.

*   **User Authentication:** Strong passwords are required for all user accounts. Passwords

meet minimum complexity requirements (e.g., minimum length, combination of uppercase, numbers, and symbols). Multifactor authentication (MFA) is recommended, where technical

* **Access Authorization:** Access to systems and data will be granted based on job role a responsibilities. Regular access reviews will be conducted to ensure that users only have ac the resources they need.

* **Account Management:** A formal process for creating, modifying, and disabling user a will be implemented. User accounts will be promptly disabled upon termination of employm change in job role.

* **Remote Access:** Remote access to systems within the low-risk environment is restric remote access is necessary, it must be secured through a Virtual Private Network (VPN) wit authentication.

* **Physical Access:** Physical access to server rooms and other sensitive areas will be restricted to authorized personnel only. Access control mechanisms (e.g., key cards, biome scanners) should be implemented where appropriate.

5. Incident Response

A simplified incident response plan will be implemented to handle security incidents effecti

* **Incident Reporting:** All employees are responsible for reporting suspected security in to [Designated Contact/Team, e.g., IT Help Desk, Security Officer].

* **Incident Classification:** Incidents will be classified based on severity and impact.

* **Incident Handling:** A defined incident handling process will be followed, including containment, eradication, recovery, and post-incident analysis.

* **Documentation:** All security incidents will be documented, including the nature of th incident, the steps taken to resolve it, and any lessons learned.

* **Escalation:** Serious security incidents will be escalated to [Designated Contact/Team further investigation and response. Legal and regulatory reporting requirements will be fol necessary.

6. Security Awareness Training

Security awareness training is crucial for promoting a security-conscious culture.

* **Frequency:** Annual security awareness training will be provided to all employees and contractors.

* **Content:** Training will cover topics such as password security, phishing awareness, prevention, data protection, and incident reporting.

* **Delivery Method:** Training can be delivered through online modules, presentations, appropriate methods.

* **Documentation:** Attendance at security awareness training will be tracked and docu

* **Phishing Simulations:** Regular phishing simulations are recommended to test emplo awareness and identify areas for improvement.

7. Compliance and Auditing

Compliance with this policy will be monitored through regular audits and reviews.

* **Policy Review:** This policy will be reviewed and updated at least annually, or more frequently if necessary, to ensure it remains relevant and effective.

* **Internal Audits:** Periodic internal audits will be conducted to assess compliance with policy and identify any gaps in security controls.

* **External Audits:** If required by regulations or contractual obligations, external audits be conducted by qualified third-party auditors.

* **Compliance Reporting:** Reports on compliance with this policy will be provided to [Designated Stakeholder, e.g., Management, Audit Committee].

* **ISO/IEC 27001 Alignment:** While not seeking formal certification, the organization wi strive to maintain alignment with relevant ISO/IEC 27001 controls for its defined scope.

8. Conclusion

This Cybersecurity Policy provides a framework for protecting information assets within the environment of [Organization Name]. Adherence to this policy is essential for maintaining t confidentiality, integrity, and availability of patient data and other sensitive information, an for complying with applicable laws and regulations. All employees and contractors are resp

for understanding and complying with this policy. Regular review and updates will ensure th
remains effective and relevant in the face of evolving threats.