# Cybersecurity Policy for Healthcare Organization (Low Risk Environment)

### 1. Introduction

This Cybersecurity Policy outlines the minimum-security requirements for [Organization Name] to protect the confidentiality, integrity, and availability of protected health information (PHI) and other sensitive data. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing [Organization Name]'s systems and data. It is designed to establish a security baseline commensurate with our identified low-risk environment while adhering to relevant compliance standards, specifically SOC 2.

This policy is a living document and will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in technology, threats, regulatory requirements, and business operations. All users are responsible for understanding and adhering to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

### 2. Risk Assessment

[Organization Name] conducts regular risk assessments to identify, evaluate, and mitigate potential threats and vulnerabilities to our systems and data. Given our determination as a low-risk environment, these assessments will focus on identifying readily addressable threats and vulnerabilities with minimal business impact.

Risk assessments will include, but are not limited to:

- --Annual Security Review:-- A comprehensive review of existing security controls, policies, and procedures.
- --Vulnerability Scanning:-- Regular automated scans of systems and networks to identify known vulnerabilities. Scans will be performed at least quarterly.
- --Threat Monitoring:-- Implementation of basic security monitoring tools and processes to detect suspicious activity.
- --Third-Party Risk Management:-- Due diligence reviews of third-party vendors with access to sensitive data, focusing on their adherence to security best practices.

Identified risks will be documented, prioritized based on likelihood and impact, and addressed through appropriate mitigation strategies. Mitigation strategies may include implementing technical controls, improving security policies and procedures, or accepting the risk based on cost-benefit analysis and business requirements.

### 3. Data Protection

[Organization Name] is committed to protecting the privacy and security of all data, especially PHI. This policy mandates the following data protection measures:

- --Data Classification:-- Data will be classified based on its sensitivity and criticality. PHI and other sensitive data will be clearly identified and protected accordingly.
- --Data Encryption:-- Encryption will be used to protect sensitive data at rest and in transit. Encryption standards must be industry-accepted and regularly updated.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed to ensure

business continuity in the event of a system failure or data loss. Backups will be stored securely and tested regularly.
- --Data Retention and Disposal:-- Data will be retained only as long as necessary for business or legal purposes and securely disposed of when no longer needed. Disposal methods will comply with applicable regulations and standards.
- --Data Loss Prevention (DLP):-- Basic DLP measures will be implemented to prevent the unauthorized disclosure of sensitive data. This may include monitoring data movement, restricting access to sensitive data, and educating users on data protection best practices.

### 4. Access Controls

Access to systems and data will be restricted to authorized personnel based on the principle of least privilege. The following access control measures will be enforced:

- --User Account Management:-- All users will be assigned unique usernames and passwords. Generic or shared accounts are prohibited.
- --Password Policy:-- Strong passwords will be required, and users will be required to change their passwords regularly. Password complexity and length requirements will be enforced.
- --Multi-Factor Authentication (MFA):-- MFA will be implemented for all users accessing sensitive systems and data remotely.
- --Role-Based Access Control (RBAC):-- Access permissions will be granted based on job roles and responsibilities. Users will only be granted access to the systems and data they need to perform their job functions.
- --Access Reviews:-- Periodic reviews of user access permissions will be conducted to ensure that access remains appropriate and necessary. Terminated employee accounts will be disabled immediately.

### 5. Incident Response

[Organization Name] will maintain an incident response plan to effectively detect, respond to, and recover from security incidents. The incident response plan will include:

- --Incident Detection and Reporting:-- Procedures for identifying and reporting security incidents. All users are responsible for reporting any suspected security incidents to the designated security contact.
- --Incident Response Team:-- A designated team responsible for managing and coordinating incident response activities.
- --Incident Containment and Eradication:-- Procedures for containing and eradicating security incidents to prevent further damage.
- --Incident Recovery:-- Procedures for restoring systems and data to their normal state after a security incident.
- --Post-Incident Analysis:-- Analysis of security incidents to identify root causes and implement corrective actions to prevent future occurrences.

The incident response plan will be tested and updated regularly to ensure its effectiveness.

### 6. Security Awareness Training

[Organization Name] will provide regular security awareness training to all employees, contractors, and vendors. Training will cover topics such as:

- --Password Security:-- Best practices for creating and managing strong passwords.
- --Phishing Awareness:-- How to identify and avoid phishing attacks.
- --Data Protection:-- Protecting sensitive data and complying with data protection policies.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks.
- --Incident Reporting:-- Procedures for reporting security incidents.

Security awareness training will be conducted at least annually and reinforced through ongoing communications and reminders.

### 7. Compliance and Auditing

[Organization Name] is committed to complying with all applicable laws, regulations, and standards, including SOC 2. The following compliance and auditing measures will be implemented:

- --SOC 2 Compliance:-- Maintain controls and processes necessary to meet the Trust Services Criteria for SOC 2.
- --Internal Audits:-- Regular internal audits will be conducted to assess compliance with this policy and identify areas for improvement.
- --External Audits:-- Periodic external audits will be conducted to verify compliance with SOC 2 and other relevant regulations.
- --Policy Enforcement:-- Management is responsible for enforcing this policy and ensuring that all users comply with its requirements.

### 8. Conclusion

This Cybersecurity Policy is essential for protecting the confidentiality, integrity, and availability of [Organization Name]'s systems and data. By adhering to this policy, we can minimize our risk exposure and ensure the continued security of our organization. This policy will be reviewed and updated regularly to reflect changes in the threat landscape, technology, and regulatory requirements. All users are responsible for understanding and complying with this policy.