Okay, here's a comprehensive cybersecurity policy tailored for a low-risk healthcare environment, incorporating NIST alignment, feedback revisions, and accessibility for various audiences.

--Cybersecurity Policy for [Healthcare Organization Name]--

--Version:-- 1.0
--Date:-- October 26, 2023
--Approved by:-- [Name and Title]
--Review Cycle:-- Annually

--1. Introduction--

--1.1 Purpose:-- This Cybersecurity Policy outlines the mandatory security requirements for [Healthcare Organization Name] (hereinafter "the Organization"). Its purpose is to protect the confidentiality, integrity, and availability of our information assets, including Protected Health Information (PHI) and other sensitive data. This policy is designed to minimize risks associated with cyber threats and ensure compliance with applicable regulations, including the Health Insurance Portability and Accountability Act (HIPAA), and industry best practices.

--1.2 Scope:-- This policy applies to all employees, contractors, vendors, volunteers, students, and any other individuals or entities who access, use, or manage the Organization's information systems, networks, and data, regardless of location. This includes but is not limited to:

- All computers, servers, mobile devices, and network equipment owned or managed by the Organization.
- All applications and software used by the Organization.
- All data, including PHI, financial data, and other sensitive information.
- Business Associate Agreements

--1.3 Policy Objectives:-- This policy aims to achieve the following objectives, mapped to the NIST Cybersecurity Framework (CSF):

- --Identify (ID):-- Establish a comprehensive understanding of the Organization's cybersecurity risk profile, including assets, threats, and vulnerabilities (ID.AM-1, ID.AM-2, ID.RA-1, ID.RA-2, ID.RA-3, ID.DE-1, ID.DE-2, ID.DE-3, ID.DE-4, ID.DE-5).
- --Protect (PR):-- Implement safeguards to protect critical infrastructure and data (PR.AC-1, PR.AC-2, PR.AC-3, PR.DS-1, PR.DS-2, PR.DS-3, PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4, PR.PT-5).
- --Detect (DE):-- Develop and implement activities to identify the occurrence of a cybersecurity event (DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.IP-1).
- --Respond (RS):-- Develop and implement activities to take action regarding a detected cybersecurity incident (RS.RP-1, RS.RP-2, RS.RP-3, RS.AN-1, RS.AN-2, RS.AN-3, RS.CO-1, RS.CO-2, RS.MI-1, RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2).
- --Recover (RC):-- Develop and implement activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident (RC.RP-1, RC.RP-2, RC.RP-3, RC.IM-1, RC.IM-2, RC.CO-1).

--2. Risk Assessment--

--2.1 Risk Management Process:-- The Organization will conduct regular risk assessments, at least annually, to identify, analyze, and evaluate cybersecurity risks. The risk assessment process will include:

- --Asset Identification:-- Identifying all critical information assets, including hardware, software, data, and personnel.
- --Threat Identification:-- Identifying potential threats that could exploit vulnerabilities in the Organization's systems and data. Examples include malware, phishing, ransomware, and insider threats.
- --Vulnerability Assessment:-- Identifying weaknesses in the Organization's systems, networks, and processes. This may include penetration testing, vulnerability scanning, and security audits.
- --Impact Assessment:-- Evaluating the potential impact of a successful cyberattack on the Organization's operations, reputation, and compliance.
- --Likelihood Assessment:-- Evaluating the likelihood of a threat exploiting a vulnerability.
- --Risk Prioritization:-- Prioritizing risks based on their potential impact and likelihood.

--2.2 Mitigation Strategies:-- Based on the risk assessment, the Organization will implement appropriate mitigation strategies to reduce the identified risks. These strategies may include:

- Implementing technical controls, such as firewalls, intrusion detection systems, and anti-malware software.
- Developing and implementing security policies and procedures.
- Providing security awareness training to employees.
- Implementing incident response plans.
- Purchasing cyber insurance.

--2.3 NIST Alignment:-- The risk assessment process will align with NIST CSF ID.RA-1: Assets are identified and managed. Specifically, the risk assessment will consider NIST Special Publication 800-30, "Guide for Conducting Risk Assessments," for guidance on performing risk assessments.

--3. Data Protection--

--3.1 Data Classification:-- All data created, processed, stored, or transmitted by the Organization will be classified according to its sensitivity and criticality. Data classifications will include:

- --Confidential:-- Data that, if disclosed without authorization, could cause significant harm to the Organization, its patients, or employees (e.g., PHI, financial records).
- --Private:-- Data that should only be accessible to authorized personnel within the organization.
- --Internal:-- Data that is intended for internal use only and is not generally available to the public.

• --Public:-- Data that is publicly available and does not require protection.

--3.2 Data Encryption:-- Confidential data will be encrypted both in transit and at rest. Encryption keys will be managed securely. Data classification will dictate the level of encryption required.

• --In Transit:-- All data transmitted over public networks, including the internet, will be encrypted using strong encryption protocols, such as TLS 1.2 or higher.
• --At Rest:-- Confidential data stored on hard drives, servers, and other storage devices will be encrypted using strong encryption algorithms, such as AES-256.

--3.3 Data Loss Prevention (DLP):-- The Organization will implement DLP measures to prevent sensitive data from leaving the Organization's control. This may include:

• Monitoring network traffic for unauthorized data transfers.
• Blocking access to unauthorized websites and applications.
• Implementing controls to prevent data from being copied to removable media.
• Implementing data masking techniques to protect sensitive data in non-production environments.

--3.4 Data Backup and Recovery:-- The Organization will maintain regular backups of all critical data. Backups will be stored offsite in a secure location. The Organization will test its backup and recovery procedures regularly to ensure that data can be restored in a timely manner.

--3.5 NIST Alignment:-- Data protection measures align with NIST CSF PR.DS-1: Data-at-rest is protected, and PR.DS-2: Data-in-transit is protected. Encryption standards and key management will adhere to guidelines found in NIST Special Publication 800-57, "Recommendation for Key Management."

--4. Access Controls--

--4.1 Least Privilege:-- Users will be granted access to only the information and systems they need to perform their job duties. Access rights will be reviewed regularly and adjusted as needed.

--4.2 Account Management:--

• --User Account Creation:-- All user accounts will be created through a formal process.
• --Password Management:-- Users will be required to create strong passwords that meet the Organization's password policy. Passwords must be complex, unique, and changed regularly. Multi-Factor Authentication (MFA) will be enabled for all critical systems.
• --Account Termination:-- When an employee or contractor leaves the Organization, their user accounts will be promptly disabled or deleted.

--4.3 Network Access Control:-- The Organization will implement network access controls to restrict access to its internal network. This includes:

• --Firewalls:-- Firewalls will be used to protect the Organization's network from unauthorized access.
• --Intrusion Detection/Prevention Systems (IDS/IPS):-- IDS/IPS will be used to monitor

network traffic for malicious activity.
- --Virtual Private Networks (VPNs):-- VPNs will be used to provide secure remote access to the Organization's network.

--4.4 Physical Access Control:-- Physical access to the Organization's facilities and computer rooms will be restricted to authorized personnel. This includes:

- --Badge Access:-- Employees and contractors will be required to use badges to access the Organization's facilities.
- --Security Cameras:-- Security cameras will be used to monitor the Organization's facilities.

--4.5 NIST Alignment:-- Access control measures align with NIST CSF PR.AC-1: Identity management, authentication, and access control. Implementation will follow recommendations found in NIST Special Publication 800-63, "Digital Identity Guidelines."

--5. Incident Response--

--5.1 Incident Response Plan:-- The Organization will maintain a written Incident Response Plan (IRP) that outlines the steps to be taken in the event of a cybersecurity incident. The IRP will be tested and updated regularly.

--5.2 Incident Reporting:-- All suspected security incidents must be reported immediately to the [Designated Contact/Team, e.g., IT Security Team].

--5.3 Incident Response Process:-- The IRP will include the following steps:

- --Detection:-- Identifying and confirming a security incident.
- --Containment:-- Limiting the scope and impact of the incident.
- --Eradication:-- Removing the cause of the incident.
- --Recovery:-- Restoring affected systems and data.
- --Post-Incident Activity:-- Analyzing the incident to identify lessons learned and improve security measures.

--5.4 Legal and Regulatory Reporting:-- The Organization will comply with all applicable legal and regulatory requirements for reporting security incidents, including HIPAA breach notification requirements.

--5.5 NIST Alignment:-- Incident response activities align with NIST CSF RS.RP-1: Response plan is developed and maintained, and RS.MI-1: Analysis is conducted to ensure adequate response. The IRP should be built based on NIST Special Publication 800-61, "Computer Security Incident Handling Guide."

--6. Security Awareness Training--

--6.1 Training Program:-- The Organization will provide regular security awareness training to all employees, contractors, and other users. Training will cover topics such as:

- Password security
- Phishing awareness
- Malware prevention

• Data protection
• Incident reporting
• Social engineering

--6.2 Training Frequency:-- Security awareness training will be provided to new employees upon hire and annually thereafter. Additional training may be provided as needed to address emerging threats or vulnerabilities.

--6.3 Phishing Simulations:-- The Organization may conduct periodic phishing simulations to test employees' awareness of phishing attacks.

--6.4 NIST Alignment:-- Security awareness training aligns with NIST CSF PR.AT-1: Users are trained and aware of cybersecurity risks. Training programs will be based on guidance found in NIST Special Publication 800-16, "Information Technology Security Training Requirements."

--7. Compliance and Auditing--

--7.1 Compliance Requirements:-- The Organization is committed to complying with all applicable laws, regulations, and industry standards, including:

• HIPAA
• HITECH Act
• [State-specific privacy laws, if applicable]

--7.2 Auditing:-- The Organization will conduct regular security audits to assess its compliance with this policy and applicable regulations. Audits will be performed by internal or external auditors.

--7.3 Continuous Monitoring:-- The Organization will establish and maintain continuous monitoring procedures to detect security events and track compliance with this policy. This will include:

• Log monitoring
• Vulnerability scanning
• Security incident reporting
• Regular review of access controls

--7.4 Policy Enforcement:-- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

--7.5 NIST Alignment:-- Compliance and auditing activities align with NIST CSF ID.GV-1: Cybersecurity policies and procedures are established and maintained. Continuous monitoring aligns with NIST CSF DE.CM-1: Detection processes and procedures are established and maintained. Audit procedures will be guided by NIST Special Publication 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations."

--8. Conclusion--

This Cybersecurity Policy is a critical component of the Organization's overall risk management strategy. By adhering to this policy, all users can help protect the

Organization's information assets and ensure the confidentiality, integrity, and availability of sensitive data. This policy will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in the threat landscape and the Organization's business environment. Questions about this policy should be directed to [Designated Contact/Team, e.g., IT Security Team].

--Responsibilities:--

- --All Employees:-- Must adhere to this policy and complete all required security awareness training.
- --Managers:-- Are responsible for ensuring that their employees are aware of and comply with this policy.
- --IT Department:-- Is responsible for implementing and maintaining the technical controls required by this policy.
- --Compliance Officer:-- Is responsible for monitoring compliance with this policy and applicable regulations.
- --Senior Management:-- Is responsible for approving and supporting the implementation of this policy.

--Amendments--

Any amendments to this policy will be reviewed and approved by [Position/Committee]. These will be communicated to all parties that this policy applies to.

--Document Control--
This is a controlled document. Any changes to this document must be approved by [Position/Committee].

--Disclaimer:-- -This is a sample policy and should be customized to fit the specific needs and requirements of your organization. Consult with legal counsel and cybersecurity professionals to ensure that your policy is compliant with all applicable laws and regulations.-