Okay, here's a comprehensive cybersecurity policy designed for a low-risk healthcare environment, incorporating the feedback provided and aligned with RMF (Risk Management Framework), and tailored for diverse audiences.

--Cybersecurity Policy for [Organization Name]--

--Version:-- 1.0
--Date Issued:-- October 26, 2023
--Effective Date:-- November 1, 2023
--Approved By:-- [Name and Title, e.g., CEO, Compliance Officer]

--1. Introduction--

This Cybersecurity Policy outlines the mandatory security requirements for [Organization Name] ("the Organization") to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data. This policy applies to all employees, contractors, vendors, volunteers, and any other individuals or entities accessing, using, or managing the Organization's information systems and data, regardless of location or device type. This policy is designed to meet compliance requirements under the Health Insurance Portability and Accountability Act (HIPAA), and aligns with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) for low-risk environments. Adherence to this policy is essential to maintaining the trust of our patients, partners, and the public. Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

- --Purpose:-- To establish a framework for safeguarding information assets against unauthorized access, use, disclosure, disruption, modification, or destruction.
- --Scope:-- This policy covers all information systems, networks, applications, devices (including but not limited to computers, laptops, tablets, smartphones), data (including PHI), and physical locations owned or controlled by the Organization, as well as those used to access or process Organization data.
- --Audience:-- This policy is written for a diverse audience, including executive leadership, clinical staff, IT personnel, and administrative employees. Jargon is minimized, and where technical terms are used, clear definitions are provided.

--2. Risk Assessment--

The Organization recognizes that maintaining a robust cybersecurity posture requires continuous risk assessment. Risk assessments are performed to identify, analyze, and evaluate potential threats and vulnerabilities that could impact the confidentiality, integrity, and availability of our data and systems.

- --Risk Assessment Frequency:-- A formal risk assessment will be conducted at least annually, or more frequently if significant changes occur in the organization's environment (e.g., new systems, new regulations, a major security incident).
- --Low-Risk Environment Definition:-- For the purposes of this policy, a "low-risk environment" is defined as one characterized by:
- --Limited PHI Volume:-- The Organization handles a relatively small volume of PHI.
- --Simple IT Infrastructure:-- The IT infrastructure is relatively straightforward,

consisting primarily of standard office productivity applications, Electronic Health Record (EHR) system, and basic network services.
- --Limited Connectivity:-- The Organization has limited connectivity to external networks beyond essential internet access.
- --Limited Mobile Device Usage:-- Employee use of mobile devices for business purposes is controlled and minimized.
- --No high-value targets:-- The data is not considered likely to be a high-value target for sophisticated attackers.

This definition is subject to change based on changes in the organization's environment or threat landscape. The risk assessment will determine if these conditions still exist, and the policy will be adjusted accordingly.

- --Risk Assessment Methodology:-- The risk assessment process will follow a recognized framework, such as NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems," tailored for a low-risk environment. This includes:
- --Identifying Assets:-- Cataloging all relevant hardware, software, data, and personnel.
- --Identifying Threats:-- Identifying potential threats, such as malware, phishing attacks, insider threats, and physical security breaches.
- --Identifying Vulnerabilities:-- Identifying weaknesses in systems, applications, and processes that could be exploited by threats.
- --Analyzing Likelihood and Impact:-- Assessing the likelihood of a threat exploiting a vulnerability and the potential impact on the organization.
- --Determining Risk Levels:-- Assigning risk levels based on the likelihood and impact assessments.
- --Developing Mitigation Strategies:-- Identifying and implementing appropriate security controls to reduce risk to acceptable levels.
- --Documentation:-- All risk assessment activities and findings will be documented, including the assets assessed, threats identified, vulnerabilities discovered, risk levels assigned, and mitigation strategies implemented.

--3. Data Protection--

Protecting the confidentiality, integrity, and availability of data is paramount. The following controls are implemented to safeguard data:

- --Data Encryption:--
- --Data at Rest:-- Encryption will be used for all sensitive data stored on electronic devices and servers. For a low-risk environment, Advanced Encryption Standard (AES) with a key length of at least 128 bits is the minimum acceptable encryption algorithm. Key management procedures will follow industry best practices, including the use of strong passwords or multi-factor authentication to protect encryption keys. Acceptable technologies for data at rest include [Specific tools or software solutions used by the organization, e.g., BitLocker, FileVault].
- --Data in Transit:-- Encryption will be used for all sensitive data transmitted over networks, including email, file transfers, and remote access connections. Transport Layer Security (TLS) version 1.2 or higher is the minimum acceptable encryption protocol for data in transit.

- --Data Backup and Recovery:-- Regular backups of all critical data will be performed to ensure business continuity in the event of a system failure, disaster, or data loss.
- --Backup Frequency:-- Backups will be performed [e.g., daily, weekly] and stored in a secure, off-site location.
- --Recovery Testing:-- Data recovery procedures will be tested at least annually to ensure their effectiveness.
- --Data Loss Prevention (DLP):-- The organization will implement measures to prevent sensitive data from leaving the organization's control without authorization. These measures may include:
- --Monitoring:-- Monitoring network traffic and endpoint devices for unauthorized data transfers.
- --Filtering:-- Filtering outbound email and web traffic to prevent the transmission of sensitive data.
- --Access Controls:-- Restricting access to sensitive data based on the principle of least privilege.
- --Data Retention and Disposal:-- Data will be retained only for as long as required by law, regulation, or business need, and then securely disposed of.
- --Retention Policy:-- A data retention policy will be established and followed, specifying the retention periods for different types of data.
- --Secure Disposal:-- Data will be securely disposed of using methods that prevent unauthorized access or recovery, such as data wiping or physical destruction of storage media.

--4. Access Controls--

Access to information systems and data will be restricted to authorized users only. The following access control measures are implemented:

- --User Authentication:--
- --Strong Passwords:-- All users are required to use strong passwords that meet the following minimum requirements:
- At least 12 characters in length
- A combination of uppercase and lowercase letters, numbers, and symbols
- Not easily guessable (e.g., not based on personal information or common words)
- --Password Management:-- Users are required to change their passwords at least every 90 days. Passwords should not be reused.
- --Multi-Factor Authentication (MFA):-- MFA is implemented for all remote access connections and privileged accounts. MFA may also be implemented for other high-risk systems or applications.
- --Authorization:--
- --Least Privilege:-- Users will be granted only the minimum level of access necessary to perform their job duties.
- --Role-Based Access Control (RBAC):-- Access rights will be assigned based on roles and responsibilities, rather than individual users.
- --Access Reviews:-- User access privileges will be reviewed periodically (at least annually) to ensure that they remain appropriate.
- --Account Management:--

- --Account Creation:-- User accounts will be created only after proper authorization and verification.
- --Account Termination:-- User accounts will be promptly disabled or terminated when employment or contract ends.
- --Account Monitoring:-- User account activity will be monitored for suspicious or unauthorized activity.

--5. Incident Response--

The Organization maintains an Incident Response Plan to effectively detect, contain, eradicate, and recover from security incidents. The Incident Response Plan will be reviewed and updated at least annually.

- --Incident Response Team:-- An Incident Response Team (IRT) will be established, consisting of representatives from IT, security, legal, and management. The IRT will be responsible for coordinating the organization's response to security incidents. Roles and responsibilities within the IRT include:
- --Incident Commander:-- Leads the incident response effort and makes key decisions.
- --Technical Lead:-- Provides technical expertise and support for incident investigation and remediation.
- --Communications Lead:-- Manages communication with internal and external stakeholders.
- --Legal Counsel:-- Provides legal advice and guidance on incident response activities.
- --Incident Reporting:-- All suspected security incidents must be reported immediately to [e.g., IT Help Desk, Security Officer]. Employees are encouraged to report any suspicious activity, even if they are not sure if it constitutes a security incident.
- --Incident Response Procedures:-- The Incident Response Plan outlines detailed procedures for responding to different types of incidents, including:
- --Malware Infections:-- Procedures for identifying, containing, and removing malware from infected systems.
- --Data Breaches:-- Procedures for investigating, containing, and mitigating data breaches, including notifying affected individuals and regulatory authorities as required by law.
- --Phishing Attacks:-- Procedures for identifying and responding to phishing attacks, including educating users about phishing scams and disabling compromised accounts.
- --Denial-of-Service (DoS) Attacks:-- Procedures for mitigating DoS attacks and restoring service availability.
- --Escalation Paths:-- The Incident Response Plan outlines escalation paths for different types of incidents, specifying when to escalate incidents to higher levels of management or external authorities. The contact information for escalation can be found [e.g., in the IT Help Desk Knowledge Base].
- --Post-Incident Activities:-- After an incident has been resolved, a post-incident review will be conducted to identify lessons learned and improve incident response procedures.

--6. Security Awareness Training--

All employees, contractors, and vendors will receive security awareness training at least annually. Training will cover topics such as:

- --Password Security:-- Creating and maintaining strong passwords.

- --Phishing Awareness:-- Identifying and avoiding phishing scams.
- --Malware Prevention:-- Preventing malware infections.
- --Data Protection:-- Protecting sensitive data.
- --Incident Reporting:-- Reporting security incidents.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks.
- --HIPAA Compliance:-- Protecting patient privacy and confidentiality.
- --Acceptable Use Policy:-- Adhering to the Organization's acceptable use policy for IT resources.

Training will be tailored to the specific roles and responsibilities of different user groups. Records of training completion will be maintained.

--7. Compliance and Auditing--

The Organization is committed to complying with all applicable laws, regulations, and standards, including HIPAA. This policy is aligned with the NIST Risk Management Framework (RMF) and the following control families:

- --Access Control (AC):-- Sections 4 of this policy outlines the implementation of AC controls, specifically AC-1, AC-2, AC-3, AC-5 and AC-6.
- --Awareness and Training (AT):-- Section 6 of this policy outlines the implementation of AT controls, specifically AT-1, AT-2, AT-3, and AT-4.
- --Audit and Accountability (AU):-- The organization will maintain audit logs of system activity and user access, in line with AU-1, AU-2, AU-3, AU-6, AU-7.
- --Configuration Management (CM):-- The organization will maintain documented and secure configurations for all systems, in line with CM-1, CM-2, CM-3, and CM-7.
- --Incident Response (IR):-- Section 5 of this policy outlines the implementation of IR controls, specifically IR-1, IR-2, IR-4, IR-5, IR-6, IR-7 and IR-8.
- --Risk Assessment (RA):-- Section 2 of this policy outlines the implementation of RA controls, specifically RA-1, RA-2, and RA-3.
- --System and Information Integrity (SI):-- The organization will implement measures to protect systems from malware and other threats, in line with SI-1, SI-2, SI-3, and SI-4.

Regular audits will be conducted to assess compliance with this policy and applicable regulations. Audit findings will be reported to management, and corrective actions will be taken to address any deficiencies.

- --Policy Review:-- This policy will be reviewed and updated at least annually, or more frequently if significant changes occur in the organization's environment or regulatory landscape.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting the Organization's information assets and maintaining the trust of our patients, partners, and the public. All employees, contractors, and vendors are responsible for understanding and complying with this policy. By working together, we can create a secure and reliable IT environment that supports our mission of providing high-quality healthcare services.

--Appendices (Optional):--

• Acceptable Use Policy
• Password Policy
• Incident Response Plan
• Data Retention Policy
• List of Security Tools and Technologies Used by the Organization

--Definitions:--

• --PHI:-- Protected Health Information as defined by HIPAA.
• --RMF:-- Risk Management Framework.
• --AES:-- Advanced Encryption Standard.
• --TLS:-- Transport Layer Security.

This revised policy provides a more specific and actionable framework for cybersecurity in a low-risk healthcare environment, while also being accessible to a wide range of audiences. Remember to tailor the bracketed placeholders with the specific information relevant to your organization. Good luck!