Okay, here's a comprehensive cybersecurity policy tailored for a low-risk healthcare environment, incorporating the provided feedback and aligned with ISO/IEC 27001. The policy aims to be understandable by both technical and non-technical audiences.

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

--Effective Date:-- October 26, 2023
--Version:-- 1.0

--1. Introduction--

--1.1 Purpose--

This Cybersecurity Policy outlines the mandatory security requirements for [Healthcare Organization Name] (hereafter referred to as "the Organization"). It is designed to protect the confidentiality, integrity, and availability of patient information, financial data, and other sensitive business assets. This policy supports our commitment to delivering high-quality healthcare services while adhering to all relevant legal, ethical, and regulatory requirements. It is aligned with the principles of ISO/IEC 27001, an internationally recognized standard for information security management systems. All employees, contractors, vendors, and other individuals accessing or using the Organization's IT resources are required to comply with this policy.

--1.2 Scope--

This policy applies to all information and IT resources owned, leased, or managed by the Organization, including but not limited to:

• All computers, servers, mobile devices, and network infrastructure.
• All electronic protected health information (ePHI) and other confidential data.
• All software applications and systems.
• All employees, contractors, vendors, and other authorized users.
• All physical locations where organizational assets are stored or operated.

--1.3 Policy Objectives--

The primary objectives of this policy are to:

• Protect patient privacy and comply with HIPAA and other relevant regulations.
• Prevent unauthorized access to sensitive data.
• Ensure the availability and integrity of critical systems and data.
• Establish clear roles and responsibilities for cybersecurity.
• Provide a framework for continuous improvement of our security posture.
• Minimize the risk of cyberattacks and data breaches.

--2. Risk Assessment--

--2.1 Methodology--

The Organization will conduct regular risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to its information assets. These assessments will be performed at least annually and more frequently as needed based on changes in the

threat landscape or within the organization. The risk assessment process will follow a recognized methodology (e.g., NIST Risk Management Framework or ISO 27005) and will include:

- --Asset Identification:-- Identifying and categorizing all information assets based on their value and sensitivity.
- --Threat Identification:-- Identifying potential threats that could exploit vulnerabilities.
- --Vulnerability Assessment:-- Identifying weaknesses in systems, applications, and processes.
- --Likelihood and Impact Analysis:-- Evaluating the likelihood and potential impact of identified risks.
- --Risk Prioritization:-- Prioritizing risks based on their severity and likelihood.

--2.2 Risk Treatment--

Based on the risk assessment results, the Organization will develop and implement risk treatment plans to:

- --Mitigate:-- Implement controls to reduce the likelihood or impact of identified risks.
- --Transfer:-- Transfer the risk to a third party (e.g., through insurance).
- --Accept:-- Accept the risk if the cost of mitigation outweighs the potential benefits (this requires senior management approval).
- --Avoid:-- Avoid the activity that creates the risk.

--3. Data Protection--

--3.1 Data Classification--

All data will be classified based on its sensitivity and criticality. The following data classifications will be used:

- --Public:-- Information that is freely available to the public.
- --Internal:-- Information intended for internal use only.
- --Confidential:-- Sensitive information that requires strict protection (e.g., patient data, financial records).
- --Restricted:-- Highly sensitive information that requires the highest level of protection (e.g., passwords, encryption keys).

--3.2 Data Handling Procedures--

Specific procedures will be implemented for handling data based on its classification. These procedures will address:

- --Storage:-- Secure storage of data, including encryption where appropriate.
- --Transmission:-- Secure transmission of data, using encryption and secure protocols.
- --Access:-- Limiting access to data based on the principle of least privilege.
- --Disposal:-- Secure disposal of data, including shredding paper documents and securely wiping electronic media.

--3.3 Data Encryption--

Encryption will be used to protect sensitive data both at rest and in transit. Encryption keys will be securely managed and protected.

--3.4 Data Backup and Recovery--

Regular backups of critical data will be performed and stored securely offsite. Disaster recovery plans will be maintained and tested regularly to ensure business continuity in the event of a system failure or disaster.

--4. Access Controls--

--4.1 User Account Management--

- All users will be assigned unique user accounts.
- Strong passwords will be required and enforced. Password policies will adhere to industry best practices (e.g., minimum length, complexity requirements, regular password changes).
- User accounts will be promptly disabled or terminated when an employee leaves the organization or changes roles.
- Multi-factor authentication (MFA) will be implemented for all remote access and for access to sensitive systems.

--4.2 Authorization--

Access to information and systems will be granted based on the principle of least privilege, meaning that users will only be granted the access necessary to perform their job duties. Access rights will be regularly reviewed and updated.

--4.3 Remote Access--

Remote access to the Organization's network and systems will be secured using VPNs and other appropriate security measures. All remote access must use MFA.

--4.4 Physical Security--

A layered approach to physical security will be implemented to protect physical assets, including servers, workstations, network infrastructure, and physical copies of sensitive information. Measures include:

- --Access Control:-- Secure areas (e.g., server rooms, data centers) will be physically secured with access control systems (e.g., keycards, biometric scanners). Access will be restricted to authorized personnel only.
- --Surveillance:-- Security cameras will be strategically placed to monitor critical areas. Recordings will be stored and reviewed periodically.
- --Environmental Controls:-- Server rooms and data centers will have appropriate environmental controls, including temperature and humidity control, fire suppression systems, and backup power.
- --Visitor Management:-- A visitor log will be maintained, and visitors will be escorted at all times.
- --Asset Tracking:-- Inventory of critical assets will be maintained and tracked regularly.
- --Security Awareness:-- Employees will be trained on physical security best practices, including reporting suspicious activity and protecting physical access badges.

--5. Incident Response--

--5.1 Incident Response Plan--

The Organization will maintain a written Incident Response Plan (IRP) that outlines the procedures for detecting, analyzing, containing, eradicating, and recovering from security incidents. The IRP will be regularly reviewed and tested.

--5.2 Incident Reporting--

All employees are required to report suspected security incidents immediately to the designated incident response team.

--5.3 Incident Handling--

The incident response team will investigate reported incidents, assess the impact, and take appropriate action to contain and remediate the incident.

--5.4 Post-Incident Review--

Following a security incident, a post-incident review will be conducted to identify lessons learned and improve the Organization's security posture.

--6. Security Awareness Training--

--6.1 Training Program--

All employees, contractors, and vendors will be required to complete security awareness training upon hire and annually thereafter. The training will cover topics such as:

• Data security and privacy.
• Password security.
• Phishing awareness.
• Malware prevention.
• Social engineering.
• Incident reporting.
• Physical security awareness.
• --Acceptable Use Policy (AUP)-- - The following will be reviewed:

--6.2 Acceptable Use Policy (AUP)--

This section outlines the permissible and prohibited uses of the Organization's IT resources. All users are responsible for adhering to this policy.

• --Permissible Uses:-- IT resources may be used for legitimate business purposes, including accessing, processing, and storing information related to patient care, administrative tasks, and research activities.
• --Prohibited Uses:-- The following activities are strictly prohibited:
• Accessing, storing, or transmitting illegal or offensive content.
• Engaging in unauthorized network scanning or penetration testing.
• Installing unauthorized software or hardware.
• Disclosing confidential information to unauthorized individuals.
• Using IT resources for personal gain or commercial activities.

• Circumventing security controls or attempting to gain unauthorized access.
• Downloading or installing software from untrusted sources.
• Sharing passwords or accounts with others.
• Using organization resources to propagate malicious code.
• --Monitoring:-- The Organization reserves the right to monitor the use of its IT resources to ensure compliance with this policy.

--6.3 Training Delivery--

Training will be delivered through a variety of methods, including online modules, classroom training, and awareness campaigns.

--7. Compliance and Auditing--

--7.1 Regulatory Compliance--

The Organization will comply with all applicable laws and regulations, including HIPAA, GDPR (if applicable), and other relevant privacy and security regulations.

--7.2 Internal Audits--

Regular internal audits will be conducted to assess compliance with this policy and other security requirements.

--7.3 External Audits--

The Organization will undergo periodic external audits to assess its security posture and compliance with industry standards (e.g., ISO/IEC 27001).

--7.4 Vulnerability Management--

The Organization will establish and maintain a vulnerability management program to identify, assess, and remediate vulnerabilities in its systems and applications.

• --Vulnerability Scanning:-- Regular vulnerability scans will be conducted on all systems and applications.
• --Vulnerability Assessment:-- Identified vulnerabilities will be assessed for their potential impact and likelihood of exploitation.
• --Remediation:-- Vulnerabilities will be remediated in a timely manner based on their severity. Patches and updates will be applied promptly.
• --Reporting:-- Vulnerability management activities will be documented and reported to management.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting the Organization's information assets and ensuring the privacy and security of patient data. All employees, contractors, and vendors are expected to adhere to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. This policy will be reviewed and updated at least annually or more frequently as needed to reflect changes in the threat landscape or within the organization.

--Policy Owner:-- [Job Title - e.g., Chief Information Security Officer (CISO)]

--Policy Approval:-- [Name and Title - e.g., CEO/Executive Director]
--Date of Approval:-- October 26, 2023

This policy provides a solid foundation for cybersecurity in a low-risk healthcare setting. Remember to tailor it to your organization's specific needs and circumstances. It's also vital to regularly review and update the policy to keep pace with evolving threats and technologies.