Here's a comprehensive cybersecurity policy tailored for a low-risk healthcare environment, aligned with COBIT, and addressing the feedback you provided.

--Cybersecurity Policy--

--1. Introduction--

- --Purpose:-- This Cybersecurity Policy (the "Policy") outlines the framework for protecting the confidentiality, integrity, and availability of sensitive information and systems belonging to [Healthcare Organization Name] (the "Organization"). It applies to all employees, contractors, vendors, volunteers, and any other individuals or entities accessing, using, or managing Organization information assets. This policy is designed to be scalable and adapt as the Organization and its risk profile evolve.
- --Scope:-- This Policy covers all information assets, including but not limited to electronic protected health information (ePHI), financial records, operational data, and intellectual property, regardless of location (on-premises, cloud, or mobile). It encompasses all information systems, networks, devices, and applications used to create, store, process, or transmit Organization data.
- --Compliance:-- This Policy aligns with applicable laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), and utilizes the COBIT framework for governance and management of information and technology. The COBIT framework helps us achieve our objectives by aligning IT processes with business goals and ensuring accountability.
- --Policy Maintenance:-- This Policy will be reviewed and updated at least annually, or more frequently as required by changes in laws, regulations, technology, or the Organization's risk environment. The [Designated Role, e.g., Security Officer, IT Director] is responsible for maintaining and updating this Policy.

--2. Risk Assessment--

- --Process:-- The Organization conducts regular risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to its information assets. Risk assessments will be performed at least annually and whenever there is a significant change to the Organization's environment (e.g., new systems, applications, or business processes).
- --Methodology:-- The risk assessment process will utilize a methodology consistent with industry best practices (e.g., NIST Risk Management Framework, ISO 27005) to:
- Identify assets and their value.
- Identify potential threats (e.g., malware, phishing, unauthorized access, natural disasters).
- Identify vulnerabilities that could be exploited by threats.
- Analyze the likelihood and impact of potential risks.
- Prioritize risks based on their severity.
- --Risk Mitigation:-- Based on the risk assessment results, the Organization will implement appropriate security controls to mitigate identified risks. Risk mitigation strategies may include:

- Implementing technical controls (e.g., firewalls, intrusion detection systems, encryption).
- Implementing administrative controls (e.g., policies, procedures, training).
- Transferring risk (e.g., insurance).
- Accepting risk (with documented justification).

- --Physical Security:-- The Organization maintains physical security measures to protect its facilities and information assets from unauthorized access, damage, or theft. These measures include:
- --Access Control:-- Limited access to facilities through keycard access, reception/security personnel, and visitor sign-in procedures.
- --Security Cameras:-- Security cameras monitoring entrances, exits, and other critical areas.
- --Environmental Controls:-- Measures to protect equipment from environmental hazards (e.g., fire suppression, climate control).
- --Visitor Management:-- All visitors are required to sign in, provide identification, and be escorted while on the premises.

--3. Data Protection--

- --Data Classification:-- The Organization classifies data based on its sensitivity and criticality, and implements appropriate security controls for each classification level. Data classifications include [Example: Public, Internal, Confidential, Restricted].

- --Data Security Measures:-- The following measures are implemented to protect data:
- --Encryption:-- Sensitive data at rest and in transit will be encrypted using industry-standard encryption algorithms. This includes ePHI, financial data, and other confidential information.
- --Data Loss Prevention (DLP):-- Monitoring and prevention measures to prevent sensitive data from leaving the Organization's control without authorization. This might include monitoring email, web traffic, and removable media.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored securely, with a documented recovery plan to ensure business continuity in the event of a data loss incident. Backups will be tested regularly.
- --Data Retention and Disposal:-- Data will be retained according to legal and regulatory requirements and the Organization's data retention policy. Data will be securely disposed of when it is no longer needed, using approved methods (e.g., shredding, degaussing, secure wiping).

- --Privacy:-- The Organization respects the privacy of patients and adheres to all applicable privacy laws and regulations, including HIPAA. Employees are trained on their responsibilities for protecting patient privacy.

--4. Access Controls--

- --Principle of Least Privilege:-- Access to information systems and data will be granted based on the principle of least privilege, meaning that users will only be granted the minimum level of access necessary to perform their job duties.

- --User Account Management:--
- Unique user accounts will be created for each individual accessing the Organization's systems.
- Strong passwords will be required and enforced. Password complexity requirements will be regularly reviewed and updated.
- Multi-factor authentication (MFA) will be implemented for all critical systems and remote access.
- User accounts will be promptly disabled or terminated when an individual leaves the Organization or changes roles.
- Regular reviews of user access rights will be conducted to ensure they remain appropriate.

- --Remote Access:-- Remote access to the Organization's network will be secured through VPNs and multi-factor authentication. Remote access policies will be enforced.

- --Network Segmentation:-- The Organization's network will be segmented to isolate sensitive systems and data from less sensitive areas.

--5. Incident Response--

- --Incident Response Plan:-- The Organization maintains a documented Incident Response Plan (IRP) to guide the response to security incidents. The IRP outlines the steps to be taken to identify, contain, eradicate, and recover from security incidents.

- --Incident Reporting:-- All employees are responsible for reporting suspected security incidents to the [Designated Role, e.g., IT Help Desk, Security Officer] immediately.

- --Incident Response Team:-- The Incident Response Team (IRT) is responsible for managing security incidents. The IRT consists of representatives from [Example: IT, Security, Legal, Management]. The IRT will follow the IRP to contain and resolve incidents.

- --Post-Incident Analysis:-- After each security incident, a post-incident analysis will be conducted to determine the root cause of the incident and identify areas for improvement. The results of the analysis will be used to update the IRP and security controls.

--6. Security Awareness Training--

- --Training Program:-- The Organization provides regular security awareness training to all employees, contractors, and vendors. Training covers topics such as:
- Phishing awareness
- Malware prevention
- Password security
- Data protection
- Social engineering
- Incident reporting
- [Add any other relevant topics]

- --Training Frequency:-- Security awareness training will be conducted at least annually and upon onboarding.

- --Training Records:-- Records of security awareness training will be maintained.

--7. Compliance and Auditing--

- --Policy Compliance:-- All employees are responsible for complying with this Cybersecurity Policy. Violations of this Policy may result in disciplinary action, up to and including termination of employment.
- --Internal Audits:-- Regular internal audits will be conducted to assess compliance with this Policy and identify areas for improvement.
- --External Audits:-- The Organization may be subject to external audits to verify compliance with applicable laws and regulations (e.g., HIPAA).
- --Third-Party Risk Management:--
- --Vendor Assessment:-- Before engaging a third-party vendor that will access, store, or process Organization data, a security risk assessment of the vendor's security practices will be conducted. This assessment will cover areas such as data security, access controls, and incident response. A basic questionnaire or review of the vendor's security documentation (e.g., SOC 2 report) can be used.
- --Contractual Requirements:-- Contracts with third-party vendors will include clauses requiring them to maintain adequate security controls and comply with applicable laws and regulations.
- --Ongoing Monitoring:-- The Organization will periodically review the security practices of its third-party vendors to ensure they continue to meet the Organization's security requirements.
- --Roles and Responsibilities:--
- --Chief Information Officer (CIO):-- Responsible for the overall direction and oversight of the Organization's cybersecurity program.
- --IT Director/Manager:-- Responsible for implementing and maintaining technical security controls.
- --Security Officer (if applicable, otherwise delegate to IT Director):-- Responsible for developing, implementing, and maintaining the Cybersecurity Policy, conducting risk assessments, and managing security incidents.
- --Data Protection Officer (DPO - if applicable based on data volumes and regulations):-- Responsible for overseeing data privacy compliance.
- --All Employees:-- Responsible for following this Cybersecurity Policy and reporting suspected security incidents.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting the Organization's information assets and ensuring the confidentiality, integrity, and availability of patient data. By adhering to this Policy, all individuals contribute to maintaining a secure environment and protecting the Organization from cyber threats. This policy will be reviewed and updated regularly to reflect changes in the threat landscape and the Organization's evolving needs.

--Approval:--

_____

[Name]
[Title]
[Date]