Okay, here's a revised cybersecurity policy tailored for a low-risk healthcare environment, addressing the evaluation feedback and aligning with NIST standards. This is designed to be comprehensive while remaining understandable for a diverse audience. Remember to consult with legal counsel and cybersecurity experts to ensure this policy meets all applicable regulations and specific organizational needs.

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

--1. Introduction--

This Cybersecurity Policy outlines the commitment of [Healthcare Organization Name] to protect the confidentiality, integrity, and availability of our patient data and organizational information. This policy applies to all employees, contractors, volunteers, and anyone accessing our systems or data. It is designed to align with the principles of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and relevant healthcare regulations (e.g., HIPAA, where applicable, even in a low-risk setting).

--1.1 Purpose--

The purpose of this policy is to establish a framework for managing cybersecurity risks within a defined "Low-Risk Environment" context, as detailed in Section 2.1. This framework will:

• Prevent unauthorized access to sensitive information.
• Ensure the accuracy and reliability of our data.
• Maintain the availability of our systems and services.
• Comply with applicable laws, regulations, and industry best practices.
• Establish clear roles and responsibilities for cybersecurity.

--1.2 Scope--

This policy applies to all information systems, devices, networks, applications, data (electronic and physical), and facilities owned or controlled by [Healthcare Organization Name], including those used by remote workers and third-party service providers.

--2. Risk Assessment--

--2.1 Low-Risk Environment Definition:--

For the purposes of this policy, [Healthcare Organization Name] defines a "Low-Risk Environment" as one where:

• --Data Sensitivity:-- Primarily manages patient administrative data and non-critical healthcare data. Storage and transmission of Protected Health Information (PHI) as defined by HIPAA is limited to [Specific Systems/Processes, e.g., appointment scheduling, billing]. Clinical data is handled via a separate, more secure system (if applicable).
• --System Criticality:-- System outages would cause minor disruptions to operations but would not directly impact patient care or safety.
• --Threat Landscape:-- Operates in a geographically low-threat area with minimal history of cyberattacks targeting similar organizations.

- --Security Controls:-- Implements foundational security controls outlined in this policy.
- --Business Operations:-- The impact of a breach of patient data is expected to be very low due to the type of data handled, and the impact to business operations is minimal.

Regular review of this definition will be conducted annually (or more frequently if significant changes occur) to ensure its continued accuracy.

--2.2 Risk Assessment Process:--

[Healthcare Organization Name] will conduct regular risk assessments (at least annually, or when significant changes occur) to identify, analyze, and prioritize potential cybersecurity risks. These assessments will follow a defined methodology, using NIST 800-30, Guide for Conducting Risk Assessments as the framework. The Risk assessment will consider the following:

- Asset Identification: Identifying all critical systems and data assets.
- Threat Identification: Recognizing potential threats to these assets (e.g., malware, phishing, insider threats).
- Vulnerability Assessment: Identifying weaknesses in our systems and processes.
- Likelihood Assessment: Estimating the probability of a successful attack.
- Impact Assessment: Determining the potential damage from a successful attack.
- Risk Prioritization: Ranking risks based on their likelihood and impact.
- Documentation: Maintaining a record of the risk assessment process and findings.

--2.3 Risk Treatment:--

Based on the risk assessment results, [Healthcare Organization Name] will implement appropriate controls to mitigate identified risks. These controls may include:

- Risk Avoidance: Eliminating the risk altogether (e.g., discontinuing a service).
- Risk Mitigation: Implementing security controls to reduce the likelihood or impact of the risk (e.g., implementing strong passwords).
- Risk Transfer: Shifting the risk to a third party (e.g., cyber insurance).
- Risk Acceptance: Accepting the risk if the cost of mitigation outweighs the potential benefit (with documented justification).

--3. Data Protection--

--3.1 Data Classification:--

All data handled by [Healthcare Organization Name] will be classified based on its sensitivity and criticality. Common classifications include:

- --Public:-- Information freely available to the public.
- --Internal:-- Information intended for internal use only.
- --Confidential:-- Sensitive information that requires strict protection (e.g., patient administrative data).

--3.2 Data Encryption:--

- --Data in Transit:-- All data transmitted over public networks (e.g., the internet) must be encrypted using industry-standard encryption algorithms such as TLS 1.2 or higher.

- --Data at Rest:-- Sensitive data stored on systems or devices must be encrypted using industry-standard encryption algorithms, such as AES-256. Full disk encryption must be used on laptops.

--3.3 Data Backup and Recovery:--

- Regular backups of critical data will be performed (at least [Frequency, e.g., daily]).
- Backup data will be stored in a secure, offsite location.
- Backup and recovery procedures will be tested regularly (at least [Frequency, e.g., annually]) to ensure their effectiveness.

--3.4 Data Retention and Disposal:--

- Data will be retained in accordance with legal and regulatory requirements and [Healthcare Organization Name]'s data retention policy.
- Data will be securely disposed of when it is no longer needed, using approved methods (e.g., secure wiping, degaussing, physical destruction).

--4. Access Controls--

--4.1 User Account Management:--

- All users must have unique usernames and strong passwords.
- Generic or shared accounts are prohibited.
- User accounts will be created, modified, and disabled promptly based on HR processes for onboarding, job changes, and offboarding.

--4.2 Password Policy:--

- Passwords must meet the following minimum requirements:
- At least 12 characters in length
- Contain a mix of uppercase and lowercase letters, numbers, and symbols.
- Not be easily guessable (e.g., based on personal information).
- Passwords should be changed every 90 days.
- Users are prohibited from sharing their passwords.
- Password complexity requirements will be enforced through system configurations.

--4.3 Access Granting, Review, and Revocation:--

- Access to systems and data will be granted based on the principle of least privilege (i.e., users will only have access to the information and resources they need to perform their job duties).
- All access requests must be approved by the [Designated Authority, e.g., Supervisor, IT Manager].
- Access permissions will be reviewed regularly (at least [Frequency, e.g., quarterly]) to ensure they remain appropriate.
- Access will be revoked immediately upon termination of employment or when job duties change.
- Onboarding and offboarding procedures will be integrated with HR processes to ensure timely access provisioning and revocation. The IT department will receive notifications from HR regarding employee status changes.

--4.4 Multi-Factor Authentication (MFA):--

- MFA will be implemented for all users accessing sensitive systems and data, including remote access. Acceptable MFA methods include [Examples, e.g., mobile authenticator apps, hardware tokens].

--5. Incident Response--

--5.1 Incident Response Plan:--

[Healthcare Organization Name] will maintain a documented Incident Response Plan (IRP) to guide the response to cybersecurity incidents. The IRP will include:

- Definitions of what constitutes a security incident.
- Roles and responsibilities of the Incident Response Team.
- Procedures for reporting security incidents.
- Steps for containing, eradicating, and recovering from incidents.
- Procedures for post-incident analysis and lessons learned.
- Contact information for external resources (e.g., law enforcement, cybersecurity vendors).

--5.2 Incident Response Team:--

The Incident Response Team (IRT) will be responsible for managing and coordinating the response to security incidents. The IRT will consist of representatives from:

- IT Department: Responsible for technical aspects of incident response (e.g., containment, eradication, recovery).
- [Designated individual from other department(s), e.g., Administration, Compliance].
- The Security Officer: Overall coordination and communication. The Security Officer is responsible for receiving reports of incidents, activating the IRT, and overseeing the implementation of the IRP.

--5.3 Incident Reporting:--

All employees, contractors, and volunteers are required to report any suspected security incidents immediately to the Security Officer.

--5.4 Incident Analysis and Lessons Learned:--

After each incident, the IRT will conduct a post-incident analysis to identify the root cause of the incident, assess the effectiveness of the response, and develop recommendations for improvement. These lessons learned will be used to update the IRP and security controls.

--6. Security Awareness Training--

--6.1 Training Program:--

[Healthcare Organization Name] will provide regular security awareness training to all employees, contractors, and volunteers. The training program will cover topics such as:

- Common cyber threats (e.g., phishing, malware, ransomware).
- Data protection policies and procedures.

• Password security best practices.
• Social engineering awareness.
• Incident reporting procedures.
• Acceptable use of technology.

--6.2 Training Frequency:--

Security awareness training will be provided to all new employees during onboarding and annually thereafter. Supplemental training will be provided as needed to address emerging threats or vulnerabilities.

--6.3 Training Effectiveness:--

The effectiveness of the security awareness training program will be evaluated through methods such as quizzes, simulations, and feedback surveys.

--7. Compliance and Auditing--

--7.1 Compliance with Applicable Laws and Regulations:--

[Healthcare Organization Name] is committed to complying with all applicable laws and regulations related to cybersecurity and data privacy, including [List specific regulations, e.g., HIPAA, state privacy laws].

--7.2 Policy Review and Updates:--

This Cybersecurity Policy will be reviewed and updated at least annually, or more frequently if significant changes occur in the threat landscape, regulatory environment, or organizational operations.

--7.3 Auditing:--

• Regular audits will be conducted to assess compliance with this policy and other security standards.
• Audits may be performed internally or by a qualified third-party auditor.
• Audit findings will be reported to senior management, and corrective actions will be taken to address any deficiencies.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting the information assets of [Healthcare Organization Name] and ensuring the confidentiality, integrity, and availability of our data. All employees, contractors, and volunteers are expected to adhere to this policy and to report any suspected security violations. By working together, we can maintain a secure environment and protect the trust placed in us by our patients and stakeholders.

--Policy Owner:-- [Name/Title of Person Responsible]
--Effective Date:-- [Date]
--Review Date:-- [Date]

--Important Considerations:--

- --Documentation is Key:-- Maintain thorough documentation of all security controls, risk assessments, incident response activities, and training programs.
- --Regular Review:-- Regularly review and update this policy to reflect changes in the threat landscape, technology, and regulatory requirements.
- --Communication:-- Communicate this policy clearly and effectively to all stakeholders.
- --Enforcement:-- Enforce this policy consistently and fairly.
- --Vendor Management:-- Extend this policy's principles to your third-party vendors through contractual agreements.

This revised policy provides a strong foundation for cybersecurity in a low-risk healthcare environment. Remember to tailor it to your specific organizational needs and context.