Okay, here's a cybersecurity policy addressing low-risk vulnerabilities in the finance industry, adhering to NIST principles. It's designed to be practical, not overly burdensome for low-risk scenarios, but still contributing to an overall robust security posture. Remember that this is a template and needs customization based on your organization's specific environment, systems, and risk appetite.

Cybersecurity Policy for Low-Risk Vulnerabilities

1. Introduction

- 1.1 Purpose: This policy outlines the organization's approach to managing and mitigati low-risk vulnerabilities to protect the confidentiality, integrity, and availability of information assets, in accordance with National Institute of Standards and Technology (NIST) Cybersecurity Framework principles. This policy is specifically designed to addre vulnerabilities that, if exploited, would have a limited impact on business operations, financial stability, reputation, or regulatory compliance.

- 1.2 Scope: This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using [Organization Name]'s information systems, data, or networks, regardless of their location. It encompasses all software, hardware, and cloud services used to store, process, or transmit organizational data.

- 1.3 Policy Objectives:
- To establish a consistent framework for identifying, assessing, and addressing low-risk vulnerabilities.
- To minimize the potential impact of low-risk vulnerabilities on business operations.
- To ensure compliance with relevant industry regulations and standards (e.g., GLBA, PC DSS, NYDFS).
- To promote a culture of security awareness and responsibility among all users.

2. Risk Assessment

- 2.1 Vulnerability Scanning: Regular vulnerability scanning will be performed on system and applications. Frequency will be determined based on the criticality of the system a the potential impact of a compromise, but at a minimum, all systems will be scanned quarterly.

- 2.2 Risk Prioritization: Vulnerabilities identified through scanning or other means will be assessed and prioritized based on the following factors:
- Likelihood: The probability of the vulnerability being exploited.
- Impact: The potential damage that could result from a successful exploit, considering factors such as data loss, financial loss, and reputational damage. Note: As the target is Low-Risk, Impact should always be assessed as having a minimal detrimental impact
- CVSS (Common Vulnerability Scoring System) Score: The CVSS score provides a standa measure of the vulnerability's severity. This score is only ONE factor in determining risk, other factors must be used.

- 2.3 Low-Risk Definition: For the purpose of this policy, a "low-risk" vulnerability is defined as one that meets ALL of the following criteria:
- CVSS score is between 0.1 and 3.9 (Low severity).
- Exploitation requires significant technical skill or specific contextual knowledge (e.g., internal network access).
- Exploitation would result in minimal impact to data confidentiality, integrity, or availability.
- Exploitation would not result in significant financial loss, reputational damage, or regulatory penalties.

- 2.4 Documentation: All identified vulnerabilities, their risk assessments, and remediatio actions will be documented in a vulnerability management system or spreadsheet.

3. Data Protection

- 3.1 Data Classification: Organizational data will be classified according to its sensitivity and criticality. Data classification will be reviewed annually.

- 3.2 Encryption: While encryption is essential, data that is considered low-risk does not need to be encrypted.

- 3.3 Data Retention: Data retention policies will be implemented to ensure that data is stored only for as long as necessary and securely disposed of when no longer needed.
- 3.4 Data Loss Prevention (DLP): DLP measures will be implemented where appropriate. risk data might be exempt from DLP controls.

4. Access Controls

- 4.1 Least Privilege: Access to systems and data will be granted on a "least privilege" basis, meaning users will only have the minimum level of access required to perform th job duties.

- 4.2 Account Management: User accounts will be created, managed, and terminated in a manner. Inactive accounts will be disabled or deleted after a defined period of inactivity.

- 4.3 Multi-Factor Authentication (MFA): MFA may not be mandated for all systems or dat is highly encouraged. Exceptions to MFA requirements will be documented and justified

- 4.4 Access Reviews: Periodic access reviews will be conducted to ensure that users hav appropriate access privileges.

5. Incident Response

- 5.1 Incident Reporting: All suspected security incidents, including potential exploitation of low-risk vulnerabilities, must be reported immediately to the IT Security team or designated incident response personnel.

- 5.2 Incident Response Plan: The organization's Incident Response Plan (IRP) will be followed in the event of a security incident. The IRP includes procedures for:
- Incident identification and reporting.
- Containment and eradication.
- Recovery.
- Post-incident analysis.

- 5.3 Escalation Procedures: Incidents involving low-risk vulnerabilities will be escalated to management if they meet specific criteria, such as evidence of active exploitation or potential for widespread impact.

- 5.4 Vulnerability Remediation Timeframes: The timeframes for remediating vulnerabilit are based on the vulnerability's risk level. While high and critical vulnerabilities require immediate remediation, low-risk vulnerabilities may be remediated within a reasonable timeframe (e.g., 90 days) or during scheduled maintenance windows.

6. Security Awareness Training

- 6.1 Training Content: Security awareness training will be provided to all employees and contractors. Training topics will include:
- Phishing awareness.
- Password security.
- Data handling procedures.
- Incident reporting.
- Awareness of common low-risk vulnerabilities (e.g., default passwords, unpatched software).

- 6.2 Training Frequency: Security awareness training will be provided at least annually a upon onboarding.

- 6.3 Phishing Simulations: Periodic phishing simulations will be conducted to assess employee awareness and identify areas for improvement.

7. Compliance and Auditing

- 7.1 Regulatory Compliance: The organization will comply with all applicable laws, regulations, and industry standards, including [List relevant regulations, e.g., GLBA, PC DSS, NYDFS, CCPA].

- 7.2 Internal Audits: Regular internal audits will be conducted to assess compliance with this policy and other security policies and procedures.

- 7.3 External Audits: Periodic external audits may be conducted by qualified third-party auditors to assess the effectiveness of the organization's security controls.

- 7.4 Policy Review: This policy will be reviewed and updated at least annually or more frequently as needed to reflect changes in the threat landscape, technology, or regulat requirements.

8. Conclusion

This Cybersecurity Policy provides a framework for managing low-risk vulnerabilities. All personnel are responsible for adhering 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 is a living document and will be updated periodically to reflect changes in the organization's risk profile, technology landscape, and regulatory requirements. Questions regarding this policy should be directed to the IT Security team

Key Considerations & Customization Points:

- Specific Finance Regulations: This policy is a template. You MUST tailor it to the specific regulations your financial institution faces (e.g., GLBA safeguards rule, NYDFS Cybersecurity Regulation, SEC Cybersecurity Proposals, PCI DSS if you handle credit ca data).
- Risk Appetite: The definition of "low-risk" needs to align with your organization's risk tolerance. Be prepared to justify your low-risk classifications to auditors.
- Vulnerability Scanning Tool Integration: If you use a vulnerability scanner, explicitly mention its name and how it integrates into your workflow.
- Remediation Timeframes: Set clear (and achievable) remediation timeframes for low-ris vulnerabilities. Document any exceptions to these timeframes.
- Ownership: Clearly define who is responsible for specific aspects of the policy (e.g., wh manages vulnerability scanning, who approves exceptions, who conducts training).
- Enforcement: Describe how the policy will be enforced and what consequences will res from non-compliance.
- Change Management: Ensure this policy aligns with your organization's change manag processes.

This detailed policy gives you a strong foundation for managing low-risk vulnerabilities while complying with NIST and industry best practices. Remember to customize it to you organization's specific needs and environment.