Okay, here's a comprehensive Cybersecurity Policy tailored for a low-risk financial environment, incorporating the requested feedback and aligning with PCI DSS requirements, along with the addition of an Acceptable Use Policy, Change Management, and Vulnerability Management sections.

--Cybersecurity Policy--

--1. Introduction--

This Cybersecurity Policy (the "Policy") outlines the mandatory standards and guidelines for protecting the confidentiality, integrity, and availability of [Company Name]'s information assets. This Policy applies to all employees, contractors, vendors, consultants, and any other individual or entity accessing or using [Company Name]'s information systems and data (collectively, "Users"). This Policy is designed to comply with applicable laws and regulations, including Payment Card Industry Data Security Standard (PCI DSS), and aims to minimize risks associated with cyber threats. Management is committed to ensuring the security of all information under our control and has implemented this policy to safeguard our information assets, protect our customers, and maintain the trust placed in us. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

--2. Risk Assessment--

[Company Name] conducts regular risk assessments to identify, analyze, and prioritize potential threats and vulnerabilities to its information assets.

- --Purpose:-- To proactively identify and manage cybersecurity risks that could impact the confidentiality, integrity, and availability of data.
- --Process:--
- Annual risk assessments are conducted, and ad-hoc assessments are performed when significant changes occur in the business or threat landscape.
- The Risk Assessment process includes:
- --Asset Identification:-- Identifying critical information assets (e.g., customer data, financial records, systems, applications).
- --Threat Identification:-- Identifying potential threats to these assets (e.g., malware, phishing, data breaches, insider threats).
- --Vulnerability Identification:-- Identifying weaknesses in systems, applications, and processes that could be exploited.
- --Impact Analysis:-- Assessing the potential business impact if a threat exploits a vulnerability.
- --Likelihood Assessment:-- Determining the probability of a threat occurring.
- --Risk Prioritization:-- Ranking risks based on impact and likelihood to determine the most critical areas of focus.
- --Mitigation Planning:-- Developing strategies to mitigate identified risks (e.g., implementing security controls, developing incident response plans).
- --Responsibility:-- The [Designated Security Officer/IT Manager] is responsible for overseeing the risk assessment process and ensuring its completion. The executive management team will review and approve the findings of each risk assessment.

- --Documentation:-- Risk assessment results, mitigation plans, and progress are documented and maintained for audit purposes.
- --Review and Update:-- The risk assessment process is reviewed and updated at least annually, or more frequently as needed, to reflect changes in the business, technology, or threat environment.

--3. Data Protection--

[Company Name] is committed to protecting the confidentiality, integrity, and availability of all data, especially sensitive data such as Personally Identifiable Information (PII) and cardholder data (CHD).

- --Data Classification:-- Data is classified based on its sensitivity and criticality. Classifications include:
- --Public:-- Information that can be freely shared.
- --Internal:-- Information intended for internal use only.
- --Confidential:-- Sensitive information that requires strict protection (e.g., PII, CHD, financial records).
- --Restricted:-- Highly sensitive information requiring the highest level of protection (e.g., encryption keys, system passwords).
- --Data Handling Procedures:--
- All data must be handled in accordance with its classification.
- Confidential and Restricted data must be encrypted at rest and in transit.
- Access to data is restricted based on the principle of least privilege (see Section 4).
- Data retention policies are in place to ensure data is retained only as long as necessary for business or legal purposes.
- Secure disposal methods are used to permanently erase data when it is no longer needed.
- --Data Loss Prevention (DLP):-- DLP measures, such as monitoring outbound communications and restricting the transfer of sensitive data, are implemented to prevent data leakage.

--4. Access Controls--

Access to [Company Name]'s systems and data is strictly controlled to prevent unauthorized access.

- --Principle of Least Privilege:-- Users are granted only the minimum level of access necessary to perform their job duties.
- --Account Management:--
- Unique user accounts are required for all individuals accessing systems and data.
- Shared accounts are prohibited.
- Strong passwords are required and must be changed regularly (at least every 90 days).
- Multi-Factor Authentication (MFA) is required for all access to sensitive systems and data, including remote access.
- Inactive accounts are disabled or deleted promptly.
- --Access Review:-- User access privileges are reviewed at least annually to ensure they remain appropriate.
- --Physical Access Controls:-- Physical access to data centers, server rooms, and other sensitive areas is restricted to authorized personnel only, utilizing methods such as

keycards, locks, and surveillance.

--5. Incident Response--

[Company Name] has a documented Incident Response Plan (IRP) to effectively manage and respond to cybersecurity incidents.

- --Purpose:-- To minimize the impact of security incidents and restore normal operations as quickly as possible.
- --Incident Response Team:-- The IRP identifies the key members of the incident response team, their roles, and responsibilities. The team includes representatives from IT, security, legal, and management.
- --Incident Detection and Reporting:-- All users are responsible for reporting suspected security incidents immediately to [Designated Contact/Help Desk].
- --Incident Classification:-- Incidents are classified based on their severity and impact.
- --Incident Containment, Eradication, and Recovery:-- The IRP outlines procedures for containing incidents, eradicating threats, and recovering affected systems and data.
- --Post-Incident Analysis:-- After each incident, a post-incident analysis is conducted to identify lessons learned and improve the IRP.
- --Incident Response Plan Testing:-- The Incident Response Plan will be reviewed and tested annually.

--6. Security Awareness Training--

[Company Name] provides regular security awareness training to all users to educate them about cybersecurity threats and best practices.

- --Purpose:-- To increase user awareness of security risks and promote a security-conscious culture.
- --Training Content:-- Training covers topics such as:
- Phishing and social engineering
- Malware prevention
- Password security
- Data protection
- Acceptable Use Policy
- Incident reporting
- --Training Frequency:-- All users are required to complete initial security awareness training upon hire and annual refresher training thereafter.
- --Training Delivery:-- Training is delivered through a combination of online modules, presentations, and other methods.
- --Training Records:-- Records of training completion are maintained for audit purposes.

--7. Compliance and Auditing--

[Company Name] is committed to complying with all applicable laws, regulations, and industry standards, including PCI DSS.

- --PCI DSS Compliance:-- [Company Name] adheres to the PCI DSS requirements for protecting cardholder data. This includes:
- Maintaining a secure network

- Protecting cardholder data
- Maintaining a vulnerability management program (See Section 9 below)
- Implementing strong access control measures (See Section 4 above)
- Regularly monitoring and testing networks
- Maintaining an information security policy
- --Internal Audits:-- Internal audits are conducted regularly to assess compliance with this Policy and other security standards.
- --External Audits:-- External audits are conducted as required by regulatory bodies or industry standards.
- --Audit Findings:-- Audit findings are addressed promptly and effectively to ensure ongoing compliance.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting [Company Name]'s information assets and maintaining the trust of our customers. All Users are expected to understand and comply with this Policy. This Policy is subject to change and will be reviewed and updated at least annually or as needed to reflect changes in the business environment, technology, or threat landscape.

--9. Acceptable Use Policy (AUP)--

This Acceptable Use Policy (AUP) defines the appropriate and responsible use of [Company Name]'s information technology resources, including but not limited to computers, networks, internet access, email, software, and data.

- --Purpose:-- To ensure the responsible and ethical use of company resources and to protect the organization from potential risks.
- --Permitted Uses:-- Company resources should be used primarily for legitimate business purposes. Limited personal use is permitted, provided it does not violate any other provisions of this AUP or interfere with job performance.
- --Prohibited Uses:-- The following activities are strictly prohibited:
- Accessing or distributing illegal or offensive content (e.g., pornography, hate speech).
- Engaging in activities that violate laws or regulations.
- Using company resources for personal financial gain or commercial purposes without authorization.
- Attempting to bypass security controls or gain unauthorized access to systems or data.
- Introducing malware or other harmful software into the network.
- Sharing passwords or accounts with others.
- Engaging in activities that could damage the company's reputation.
- Excessive personal use that interferes with work performance or burdens network resources.
- Downloading or installing unauthorized software.
- Circumventing or attempting to circumvent security measures.
- --Email and Internet Usage:--
- Email should be used professionally and responsibly.
- Users should be cautious of phishing emails and other scams.
- Internet access should be used primarily for business purposes.
- Downloading large files or streaming media should be done responsibly to avoid impacting

network performance.
- --Social Media Usage:-- Employees should exercise caution when using social media, and avoid posting anything that could damage the company's reputation or violate confidentiality agreements. Users are responsible for ensuring they comply with the company's social media policy.
- --Monitoring:-- [Company Name] reserves the right to monitor the use of its IT resources to ensure compliance with this AUP and to investigate potential security incidents.
- --Enforcement:-- Violations of this AUP may result in disciplinary action, up to and including termination of employment or contract.

--10. Change Management--

[Company Name] has implemented a Change Management process to control and secure changes to systems and applications.

- --Purpose:-- To minimize the risk of disruptions, errors, and security vulnerabilities associated with changes to IT systems and applications.
- --Change Request Process:-- All changes to systems and applications must be submitted through a formal change request process.
- --Change Approval:-- Change requests must be reviewed and approved by the appropriate stakeholders, including IT, security, and business representatives. The level of approval required depends on the risk and impact of the change.
- --Change Testing:-- Changes must be thoroughly tested in a non-production environment before being implemented in production.
- --Change Implementation:-- Changes must be implemented according to a documented plan, with appropriate rollback procedures in place.
- --Change Documentation:-- All changes must be documented, including the reason for the change, the implementation plan, the testing results, and the date of implementation.
- --Emergency Changes:-- Emergency changes are handled through an expedited process, but still require appropriate authorization and documentation.
- --Change Review:-- Changes are reviewed after implementation to ensure they were successful and did not introduce any new issues or vulnerabilities.
- --Roles and Responsibilities:-- Roles and responsibilities within the Change Management process are clearly defined.

--11. Vulnerability Management--

[Company Name] has established a Vulnerability Management program to identify, assess, and remediate vulnerabilities in its systems and applications.

- --Purpose:-- To reduce the organization's exposure to cyber threats by proactively identifying and addressing security vulnerabilities.
- --Vulnerability Scanning:--
- Regular vulnerability scans are conducted on all systems and applications, both internal and external facing, at least quarterly, and more frequently for critical systems.
- Authenticated scanning is used to provide more accurate vulnerability assessments.
- Web application vulnerability scanning is performed on all public-facing web applications.
- --Vulnerability Assessment:--

- Vulnerabilities are assessed based on their severity and potential impact.
- Common Vulnerability Scoring System (CVSS) scores are used to prioritize vulnerabilities.
- --Patch Management:--
- Security patches are applied to systems and applications in a timely manner.
- A documented patch management process is in place.
- Critical security patches are applied within [Define timeframe, e.g., 72 hours] of release.
- Non-critical patches are applied within [Define timeframe, e.g., 30 days].
- --Vulnerability Remediation:--
- Vulnerabilities are remediated through patching, configuration changes, or other appropriate measures.
- A remediation plan is developed for each identified vulnerability.
- Remediation efforts are tracked and monitored.
- --Exception Management:--
- Exceptions to the vulnerability management policy are documented and approved by [Designated Authority].
- Compensating controls are implemented when vulnerabilities cannot be immediately remediated.
- --Reporting:--
- Vulnerability management reports are generated regularly and provided to management.
- Reports include information on identified vulnerabilities, remediation status, and exception management.
- --Penetration Testing:--
- Periodic penetration testing is conducted to simulate real-world attacks and identify vulnerabilities that may not be detected by automated scanning. Penetration tests are performed at least annually or whenever significant changes are made to the network or systems.

--Important Considerations and Customization:--

- --Specificity:-- Replace bracketed placeholders (e.g., `[Company Name]`, `[Designated Security Officer/IT Manager]`, `[Designated Contact/Help Desk]`, `[Designated Authority]`) with specific information relevant to your organization.
- --Scope:-- Tailor the specific controls and procedures outlined in the policy to your organization's specific risk profile and business operations. For example, the frequency of scanning, acceptable personal use, and response times for vulnerabilities will depend on your risk tolerance.
- --Legal Review:-- Have the policy reviewed by legal counsel to ensure it complies with all applicable laws and regulations.
- --Accessibility:-- Ensure that the policy is easily accessible to all users.
- --Enforcement:-- Enforce the policy consistently and fairly.
- --Documentation:-- Maintain detailed records of all security activities, including risk assessments, vulnerability scans, incident responses, and audit findings.

This revised Cybersecurity Policy provides a comprehensive framework for protecting your organization's information assets, aligning with PCI DSS requirements, and addressing the feedback provided. Remember that this is a template and needs to be adapted to your

specific environment. Good luck!