Okay, here's a sample Cybersecurity Policy addressing the defined risk level and complyi with PCI DSS requirements. I'll prioritize simplicity and effectiveness suitable for a "Low" risk scenario, but still address the core principles of PCI DSS.

Important Disclaimer: This is a sample policy and requires customization for your specific organizational environment, technology infrastructure, and cardholder data handling procedures. Consult with legal counsel and cybersecurity professionals to ensure full compliance with PCI DSS and other relevant regulations.

Cybersecurity Policy for [Your Company Name]

1. Introduction

This Cybersecurity Policy outlines the essential security practices and procedures implemented by [Your Company Name] to protect our information assets, maintain the confidentiality, integrity, and availability of our systems, and comply with applicable laws and regulations, including the Payment Card Industry Data Security Standard (PCI DSS).

This policy is designed to address risks commensurate with our current threat landscape We have identified a "Low" overall risk profile, meaning our exposure to significant cyber threats is relatively limited due to [Briefly State Reason: e.g., limited online transactions, outsourced payment processing, robust network segmentation]. However, a employees, contractors, and other authorized users must adhere to this policy to ensure continuous security posture improvement and risk mitigation.

2. Risk Assessment

[Your Company Name] conducts regular risk assessments to identify, evaluate, and prioritize potential cybersecurity threats and vulnerabilities.

- Frequency: Risk assessments are conducted annually and whenever there are significa changes to our business operations, technology infrastructure, or threat landscape.
- Scope: Risk assessments cover all systems and processes that handle, store, or transm sensitive data, including cardholder data.
- Methodology: Risk assessments are performed using a methodology that considers bot likelihood and impact of potential threats. A simple qualitative assessment, such as High, Medium, Low, is deemed appropriate.
- Low-Risk Focus: Given our current "Low" risk profile, the primary focus of our risk assessments is to ensure basic security controls are effectively implemented and maintained. This includes vulnerability scanning (at least quarterly) of internet-facing systems and periodic review of security configurations.
- Remediation: Identified vulnerabilities are addressed promptly based on their severity a potential impact. A tracking system (e.g., a spreadsheet) is used to monitor remediatio efforts.

3. Data Protection

Data protection is critical to our business operations and compliance efforts. This section outlines our data protection measures for all data types, with special attention to cardholder data (CHD) if applicable.

- Data Classification: Data is classified according to its sensitivity and business value. For example: Public, Internal, Confidential, Restricted.
- Data Encryption: Sensitive data, especially cardholder data if applicable, must be encrypted both in transit and at rest. Strong encryption algorithms are required.
- Data Storage: CHD is minimized where possible and stored securely with restricted acc Retention policies are defined and enforced to ensure data is not retained longer than necessary.

- Data Disposal: Secure methods are used to dispose of data, including wiping, shredding degaussing, to prevent unauthorized access.
- PCI DSS Specifics (If Applicable): If [Your Company Name] handles cardholder data, the following specific measures must be implemented:
- Protect Stored Cardholder Data: Sensitive Authentication Data (SAD) (e.g., CVV2, PIN) n NEVER be stored. Primary Account Numbers (PAN) should be masked or truncated whe displayed (unless there is a business justification and strong security controls in place).
- Encrypt Transmission of Cardholder Data Across Open, Public Networks: Strong encrypt protocols (e.g., TLS 1.2 or higher) must be used to protect CHD during transmission ove public networks.

4. Access Controls

Access to systems and data is restricted to authorized users based on the principle of least privilege.

- User Authentication: Strong passwords are required for all user accounts. Multi-factor authentication (MFA) is encouraged for all systems, especially those containing sensitiv data or used for administrative access.
- Account Management: User accounts are created, modified, and terminated promptly b employee status and job responsibilities. Regular reviews of user access rights are conducted.
- Access Control Lists (ACLs): Access to systems and data is controlled through the use o Access Control Lists (ACLs) and other access control mechanisms.
- Remote Access: Remote access to our network and systems is strictly controlled and requires strong authentication and encryption. A Virtual Private Network (VPN) is used for secure remote access.

- Physical Access: Physical access to our facilities and systems is controlled through the use of access badges, security cameras, and other physical security measures.

5. Incident Response

[Your Company Name] has established an incident response plan to effectively manage a respond to security incidents.

- Incident Reporting: All suspected security incidents must be reported immediately to [Designated Contact: e.g., IT Department, Security Officer].
- Incident Response Team: An incident response team will be formed to investigate and respond to security incidents.
- Incident Containment: Immediate steps will be taken to contain the incident and preve further damage.
- Incident Eradication: The root cause of the incident will be identified and eliminated.
- Incident Recovery: Systems and data will be restored to normal operation.
- Post-Incident Review: A post-incident review will be conducted to identify lessons learned and improve our security posture.
- Escalation: The plan includes defined escalation paths for critical incidents.

6. Security Awareness Training

All employees, contractors, and other authorized users are required to participate in security awareness training.

- Frequency: Security awareness training is provided annually and whenever there are significant changes to our security policies or procedures.
- Content: Security awareness training covers topics such as:
- Password security
- Phishing awareness

- Malware prevention
- Data protection
- Incident reporting
- Social engineering
- Delivery: Training can be delivered through online modules, in-person sessions, or othe methods.
- Tracking: Completion of security awareness training is tracked and monitored.

7. Compliance and Auditing

[Your Company Name] is committed to complying with all applicable laws and regulation including PCI DSS.

- PCI DSS Compliance: We maintain PCI DSS compliance by implementing and maintaini security controls outlined in this policy.
- Internal Audits: Regular internal audits are conducted to assess our compliance with th policy and PCI DSS requirements.
- External Audits: An annual self-assessment questionnaire (SAQ) will be completed for P DSS compliance. If required by our acquiring bank, we will engage a Qualified Security Assessor (QSA) to conduct an independent audit.
- Policy Review: This policy will be reviewed and updated at least annually or whenever there are significant changes to our business operations, technology infrastructure, or regulatory requirements.
- Documented Evidence: Evidence of policy compliance (e.g., training records, audit repo vulnerability scan results) are maintained.

8. Conclusion

This Cybersecurity Policy is essential for protecting our information assets and

maintaining the trust of our customers and partners. All employees, contractors, and oth
authorized users 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 o
contract.

This policy is a living document and will be updated periodically to reflect changes in the threat landscape, technology, and regulatory requirements.

Signed: _____

[Name and Title of CISO/Responsible Party]

Date: _____