Okay, here's a comprehensive Cybersecurity Policy tailored for a low-risk Finance environment, adhering to PCI DSS compliance, and designed to be accessible to both technical and non-technical audiences. I've tried to balance comprehensiveness with clarity, acknowledging the "low risk" context while still maintaining the necessary rigor for the Finance industry.

--Cybersecurity Policy--

--1. Introduction--

--1.1 Purpose:--

This Cybersecurity Policy outlines the principles, standards, and procedures that [Company Name] uses to protect its information assets, including customer data, financial records, and intellectual property, from unauthorized access, use, disclosure, disruption, modification, or destruction. The policy aims to ensure the confidentiality, integrity, and availability of our data while complying with applicable laws, regulations, and industry standards, specifically the Payment Card Industry Data Security Standard (PCI DSS).

--1.2 Scope:--

This policy applies to all employees, contractors, vendors, consultants, and any other individuals or entities accessing, using, or managing [Company Name]'s information assets. It covers all systems, networks, devices, and data, regardless of location, ownership, or method of access.

--1.3 Policy Objectives:--

• To safeguard customer data and maintain PCI DSS compliance.
• To establish a secure environment that protects the organization's information assets.
• To prevent and detect cybersecurity incidents promptly.
• To minimize the impact of any security breaches that may occur.
• To ensure the ongoing security of the organization through continuous improvement.

--1.4 Policy Review:--

This policy will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in the threat landscape, regulatory requirements, or business operations. The [Designated Security Officer/Team] is responsible for maintaining and updating this policy.

--2. Risk Assessment--

--2.1 Risk Assessment Process:--

[Company Name] will conduct regular risk assessments to identify, analyze, and prioritize cybersecurity risks. These assessments will evaluate potential threats, vulnerabilities, and the likelihood and impact of security incidents.

--2.2 Risk Assessment Frequency:--

Risk assessments will be conducted at least annually, and whenever there are significant

changes to the IT infrastructure, business processes, or regulatory requirements. Examples of significant changes include new software, new hardware, organizational restructuring, or changes in compliance requirements.

--2.3 Risk Treatment:--

Identified risks will be addressed through appropriate risk treatment strategies, including:

- --Risk Avoidance:-- Eliminating the risk by discontinuing the activity or process.
- --Risk Mitigation:-- Implementing security controls to reduce the likelihood or impact of the risk.
- --Risk Transfer:-- Transferring the risk to a third party through insurance or outsourcing agreements.
- --Risk Acceptance:-- Accepting the risk when the cost of mitigation outweighs the potential impact.
- --PCI DSS Specific Risk Assessment:-- The annual risk assessment will specifically address PCI DSS requirements and how those requirements are being met, including documentation and evidence of procedures.

--2.4 Documentation:--

All risk assessments, findings, and risk treatment plans will be documented and maintained by the [Designated Security Officer/Team].

--3. Data Protection--

--3.1 Data Classification:--

Data will be classified based on its sensitivity and criticality. Common data classifications include:

- --Public:-- Information freely available to the public.
- --Internal:-- Information intended for internal use only.
- --Confidential:-- Sensitive information that requires protection from unauthorized access, such as customer data or financial records.
- --Restricted:-- Highly sensitive information that requires the highest level of protection, such as passwords or encryption keys.

--3.2 Data Security Measures:--

Appropriate security measures will be implemented to protect data based on its classification. These measures may include:

- --Encryption:-- Encrypting sensitive data both in transit and at rest. All cardholder data must be encrypted according to PCI DSS standards.
- --Access Controls:-- Limiting access to data based on the principle of least privilege (see Section 4).
- --Data Loss Prevention (DLP):-- Implementing DLP measures to prevent sensitive data from leaving the organization's control. (Note: may not be necessary in a -low- risk environment, but should be considered if sensitive data is frequently handled.)

• --Data Backup and Recovery:-- Regularly backing up data and testing recovery procedures.
• --Secure Disposal:-- Securely disposing of data when it is no longer needed.
• --Tokenization or Masking:-- Masking or tokenizing cardholder data to reduce risk.

--3.3 Cardholder Data Protection (PCI DSS):--

[Company Name] will comply with all applicable PCI DSS requirements for protecting cardholder data. This includes:

• Maintaining a secure network.
• Protecting cardholder data.
• Maintaining a vulnerability management program.
• Implementing strong access control measures.
• Regularly monitoring and testing networks.
• Maintaining an information security policy.

--3.4 Data Retention and Disposal:--

Data will be retained only for as long as necessary to meet business and legal requirements. When data is no longer needed, it will be securely disposed of in accordance with established procedures.

--4. Access Controls--

--4.1 User Account Management:--

• Unique user accounts will be created for each individual accessing [Company Name]'s systems and data.
• Generic or shared accounts are prohibited, with limited exceptions that must be documented and approved by the [Designated Security Officer/Team].
• Strong passwords will be required and enforced. Password complexity requirements will be regularly reviewed and updated.
• Multi-factor authentication (MFA) will be implemented where feasible, especially for accessing sensitive systems and data (e.g., cardholder data environments).
• User accounts will be promptly disabled or terminated when employees leave the organization or change roles.

--4.2 Least Privilege:--

Access to systems and data will be granted based on the principle of least privilege. Users will only be granted the access necessary to perform their job duties.

--4.3 Access Control Lists (ACLs):--

Access control lists will be used to restrict access to files, directories, and other resources.

--4.4 Physical Security:--

Physical access to data centers and other sensitive areas will be restricted to authorized personnel. Access will be controlled through measures such as key cards, biometric scanners, or security guards.

--4.5 Remote Access:--

Remote access to [Company Name]'s systems and data will be secured through the use of Virtual Private Networks (VPNs) and multi-factor authentication.

--5. Incident Response--

--5.1 Incident Response Plan:--

[Company Name] maintains a documented Incident Response Plan (IRP) that outlines the procedures for responding to cybersecurity incidents.

--5.2 Incident Response Team:--

An Incident Response Team (IRT) will be responsible for managing and coordinating incident response activities. The IRT will include representatives from IT, security, legal, and communications.

--5.3 Incident Reporting:--

All employees, contractors, and vendors are required to report suspected security incidents immediately to the [Designated Security Officer/Team] or the IRT.

--5.4 Incident Response Process:--

The incident response process will typically involve the following steps:

1. --Detection:-- Identifying and verifying the incident.
2. --Containment:-- Isolating the affected systems and data to prevent further damage.
3. --Eradication:-- Removing the malware or other cause of the incident.
4. --Recovery:-- Restoring systems and data to normal operation.
5. --Post-Incident Analysis:-- Analyzing the incident to determine the root cause and identify areas for improvement.
6. --Communication:-- Communicating the incident to affected parties, as appropriate.

--5.5 Documentation:--

All security incidents will be documented, including the date, time, nature of the incident, and the actions taken to resolve it.

--5.6 Escalation:--

Serious incidents will be escalated to senior management and, if required, to law enforcement or regulatory agencies.

--6. Security Awareness Training--

--6.1 Training Program:--

[Company Name] will provide regular security awareness training to all employees, contractors, and vendors.

--6.2 Training Content:--

The training will cover topics such as:

• Identifying and avoiding phishing attacks.
• Password security best practices.
• Data protection policies and procedures.
• Social engineering awareness.
• Incident reporting procedures.
• Acceptable use of company resources.
• PCI DSS awareness (for personnel handling cardholder data).

--6.3 Training Frequency:--

Security awareness training will be conducted at least annually and whenever there are significant changes to the security landscape or company policies. New employees will receive training upon hire.

--6.4 Training Records:--

Records of training completion will be maintained by the [Designated Security Officer/Team].

--7. Compliance and Auditing--

--7.1 Compliance Requirements:--

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

--7.2 Internal Audits:--

Regular internal audits will be conducted to assess compliance with this Cybersecurity Policy and other relevant security standards.

--7.3 External Audits:--

Periodic external audits will be conducted by qualified third-party auditors to verify compliance with PCI DSS and other applicable regulations. This will include annual self-assessment questionnaires and, potentially, onsite assessments depending on transaction volume.

--7.4 Remediation:--

Any identified compliance gaps or security vulnerabilities will be promptly remediated.

--7.5 Documentation:--

All compliance activities, audit results, and remediation plans will be documented and maintained by the [Designated Security Officer/Team].

--8. Conclusion--

This Cybersecurity Policy is essential for protecting [Company Name]'s information assets and ensuring the confidentiality, integrity, and availability of our data. All employees, contractors, and vendors are responsible for adhering to this policy and reporting any suspected security violations. By working together, we can create a secure environment that protects our business, our customers, and our reputation.

--Policy Owner:-- [Name and Title of Policy Owner - e.g., Chief Information Officer]

--Date of Last Revision:-- [Date]

--Next Review Date:-- [Date]

--Key Improvements Incorporated:--

- --Clarity for all audiences:-- The language is simplified and explanations are provided for technical terms.
- --Specific PCI DSS References:-- The policy includes explicit references to PCI DSS requirements in relevant sections.
- --Risk-Based Approach:-- Emphasis on risk assessment and tailoring security measures to the level of risk.
- --Incident Response Detail:-- Expanded on the incident response process.
- --Regular Review:-- Reinforced the importance of regular policy review and updates.
- --Designated Responsibility:-- Clearly defined roles and responsibilities for key aspects of the policy.
- --Adaptability:-- The policy can be adapted for business needs.

Remember to customize this policy to fit your specific organization's structure, technology, and risk profile. Consider having legal counsel review it as well.