Cybersecurity Policy for a Low-Risk Financial Environment

--1. Introduction--

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of information assets within our organization. This policy is designed to address the specific security needs of our low-risk environment within the finance industry, while adhering to relevant regulatory requirements, including Payment Card Industry Data Security Standard (PCI DSS). All employees, contractors, vendors, and other authorized users are required to comply with this policy. Its goal is to foster a culture of security awareness and responsibility, mitigating potential risks and maintaining the trust of our customers and stakeholders.

--2. Risk Assessment--

We conduct regular risk assessments to identify, analyze, and prioritize potential threats and vulnerabilities to our information assets. These assessments, performed at least annually and following any significant change to our environment, consider factors such as:

- --Asset criticality:-- The business impact of the compromise of a specific asset.
- --Threat landscape:-- Potential threats, including malware, phishing, social engineering, and insider threats.
- --Vulnerability analysis:-- Weaknesses in our systems, applications, and processes.
- --Likelihood and Impact:-- The probability of a threat exploiting a vulnerability and the potential business impact.

Risk assessment results are used to inform the development and implementation of appropriate security controls and prioritize remediation efforts. Given our low-risk profile, we focus on foundational security controls and preventative measures to minimize the likelihood of successful attacks.

--3. Data Protection--

Data protection is paramount. The following measures are in place to safeguard sensitive information:

- --Data Classification:-- Data is classified based on its sensitivity and criticality (e.g., Public, Internal, Confidential, Restricted). Appropriate security controls are applied based on classification.
- --Data Encryption:-- Sensitive data, including cardholder data (CHD) covered by PCI DSS, must be encrypted both in transit and at rest using industry-standard encryption algorithms.
- --Data Masking and Tokenization:-- Cardholder data must be masked when displayed and tokenized when stored or transmitted internally where full card numbers are not required for business purposes, following PCI DSS guidelines.
- --Data Retention and Disposal:-- Data retention policies define how long data is stored and procedures for secure disposal of data no longer needed. Data disposal methods must render the data unrecoverable.
- --Data Loss Prevention (DLP):-- While our environment is low risk, basic DLP measures,

such as monitoring outbound email for sensitive keywords, are implemented to prevent accidental or malicious data leakage.

--4. Access Controls--

Access to systems and data is granted based on the principle of least privilege, ensuring that users only have the access necessary to perform their job duties.

- --User Authentication:-- Strong authentication methods, such as multi-factor authentication (MFA) where feasible and mandated by PCI DSS, are required for accessing sensitive systems and data. Complex passwords and regular password changes are enforced.
- --Access Control Lists (ACLs):-- Access control lists are used to restrict access to specific files and directories based on user roles and responsibilities.
- --Role-Based Access Control (RBAC):-- User access is managed through roles, simplifying administration and ensuring consistent access privileges.
- --Regular Access Reviews:-- Access privileges are reviewed regularly (at least annually) to ensure that users have the appropriate level of access. Terminated employees' access is revoked immediately.
- --Physical Security:-- Physical access to server rooms and other sensitive areas is restricted and monitored.

--5. Incident Response--

A well-defined incident response plan is crucial for minimizing the impact of security incidents.

- --Incident Response Plan:-- A documented incident response plan outlines the steps to be taken in the event of a security incident, including identification, containment, eradication, recovery, and post-incident analysis.
- --Incident Reporting:-- All employees are responsible for reporting suspected security incidents to the designated security contact or IT department.
- --Incident Analysis:-- Security incidents are thoroughly investigated to determine the root cause and prevent future occurrences.
- --Communication:-- Communication protocols are established to ensure timely and effective communication during a security incident, both internally and externally (e.g., to customers, regulatory agencies).
- --Regular Testing:-- The incident response plan is tested regularly through tabletop exercises or simulations to ensure its effectiveness.

--6. Security Awareness Training--

Security awareness training is provided to all employees to educate them about potential security threats and best practices.

- --Annual Training:-- All employees receive annual security awareness training covering topics such as phishing, malware, social engineering, password security, and data protection.
- --Phishing Simulations:-- Phishing simulations are conducted to test employees' ability to identify and report phishing attempts.
- --Regular Updates:-- Security awareness training is updated regularly to address emerging

threats and vulnerabilities.
- --Role-Based Training:-- Targeted training is provided to employees with specific security responsibilities (e.g., developers, system administrators).

--7. Compliance and Auditing--

We maintain compliance with applicable laws, regulations, and industry standards, including PCI DSS.

- --PCI DSS Compliance:-- We adhere to all applicable PCI DSS requirements for protecting cardholder data, including regular vulnerability scanning, penetration testing, and security assessments.
- --Internal Audits:-- Internal audits are conducted regularly to assess compliance with this Cybersecurity Policy and other security standards.
- --External Audits:-- External audits are conducted by qualified security assessors (QSAs) to validate PCI DSS compliance.
- --Policy Updates:-- This Cybersecurity Policy is reviewed and updated at least annually or as needed to address changes in the threat landscape, regulatory requirements, or business operations.
- --Documentation:-- Security policies, procedures, and controls are documented and maintained.

--8. Conclusion--

This Cybersecurity Policy demonstrates our commitment to protecting our information assets and maintaining a secure environment. By adhering to this policy, we can minimize our risk exposure, maintain compliance with applicable regulations, and preserve the trust of our customers and stakeholders. All employees are expected to actively participate in maintaining a strong security posture and reporting any security concerns. Continuous improvement and adaptation are essential to effectively address the evolving threat landscape.