Cybersecurity Policy for a Low-Risk Finance Environment

--1. Introduction--

This Cybersecurity Policy outlines the essential security measures implemented to protect the confidentiality, integrity, and availability of information assets within our organization. Recognizing the sensitivity of financial data and the importance of maintaining customer trust, this policy is designed to establish a secure operating environment, aligned with industry best practices and relevant compliance standards, specifically PCI DSS, while acknowledging our assessment as a Low-Risk entity. All employees, contractors, and third-party vendors are responsible for adhering to this policy.

--2. Risk Assessment--

Although classified as a low-risk environment, primarily due to limited scope and transaction volume, regular risk assessments are conducted to identify and evaluate potential threats and vulnerabilities to our information assets. These assessments consider factors such as:

- --Asset criticality:-- Classifying data and systems based on their importance to business operations and potential impact of compromise.
- --Threat landscape:-- Monitoring emerging cyber threats and vulnerabilities specific to the financial sector and our technology stack.
- --Vulnerability scanning:-- Regularly scanning systems for known vulnerabilities and misconfigurations.
- --Impact analysis:-- Evaluating the potential impact of security breaches, including financial loss, reputational damage, and regulatory penalties.

The results of these risk assessments are used to prioritize security controls and inform ongoing security improvements. Mitigation strategies focus on implementing cost-effective controls appropriate for the identified risks.

--3. Data Protection--

Protecting sensitive data is paramount. This policy incorporates the following data protection measures:

- --Data Minimization:-- Collecting and storing only the minimum amount of data necessary for business operations.
- --Data Encryption:-- Encrypting sensitive data at rest and in transit, using strong encryption algorithms. Specifically, encryption must be implemented for all Cardholder Data (CHD) both in storage and during transmission over open, public networks, as required by PCI DSS.
- --Data Masking:-- Masking or redacting sensitive data when displayed or used in non-production environments.
- --Data Retention:-- Establishing data retention policies that comply with legal and regulatory requirements, and securely disposing of data when it is no longer needed.
- --Secure Data Handling:-- Following secure coding practices to prevent vulnerabilities such as SQL injection and cross-site scripting.

--4. Access Controls--

Access to systems and data is restricted based on the principle of least privilege. The following access control measures are implemented:

- --User Authentication:-- Enforcing strong password policies, including minimum password length, complexity requirements, and regular password changes. Multi-factor authentication (MFA) is required for privileged accounts and remote access, aligned with PCI DSS requirements for strong authentication.
- --Authorization:-- Granting users only the access rights necessary to perform their job duties.
- --Role-Based Access Control (RBAC):-- Assigning access rights based on job roles, simplifying access management and reducing the risk of unauthorized access.
- --Regular Access Reviews:-- Periodically reviewing user access rights to ensure they remain appropriate and revoking access for terminated employees promptly.
- --Physical Security:-- Implementing physical security controls, such as access badges and surveillance cameras, to protect data centers and other sensitive areas.

--5. Incident Response--

A well-defined incident response plan is essential for effectively handling security incidents. The incident response plan outlines the following:

- --Incident Detection:-- Monitoring systems for suspicious activity and establishing clear reporting procedures for potential security incidents.
- --Incident Containment:-- Isolating affected systems to prevent further damage.
- --Incident Eradication:-- Removing the root cause of the incident.
- --Incident Recovery:-- Restoring systems and data to their normal state.
- --Post-Incident Analysis:-- Conducting a post-incident review to identify lessons learned and improve security controls. All security events related to cardholder data will be logged and reviewed periodically.

--6. Security Awareness Training--

Security awareness training is provided to all employees, contractors, and third-party vendors to educate them about cybersecurity threats and best practices. Training covers topics such as:

- --Phishing awareness:-- Recognizing and avoiding phishing emails and other social engineering attacks.
- --Password security:-- Creating and maintaining strong passwords.
- --Data handling:-- Protecting sensitive data from unauthorized access or disclosure.
- --Incident reporting:-- Reporting suspected security incidents promptly.
- --Policy Compliance:-- Understanding and adhering to this Cybersecurity Policy.

Training is conducted at least annually and reinforced through regular communications and reminders.

--7. Compliance and Auditing--

This Cybersecurity Policy is designed to comply with relevant industry regulations and standards, including PCI DSS. We will:

- --Maintain PCI DSS Compliance:-- Implement and maintain all applicable PCI DSS requirements, including regular vulnerability scanning, penetration testing, and security audits.
- --Conduct Internal Audits:-- Regularly conduct internal audits to assess the effectiveness of security controls and identify areas for improvement.
- --Engage Third-Party Auditors:-- Engage qualified third-party auditors to conduct independent security assessments and validate compliance with relevant regulations and standards.
- --Document Security Controls:-- Maintain documentation of all security controls and procedures.

--8. Conclusion--

This Cybersecurity Policy is a living document that will be reviewed and updated regularly to reflect changes in the threat landscape, technology, and regulatory requirements. All employees, contractors, and third-party vendors are responsible for adhering to this policy and contributing to a secure operating environment. By implementing these security measures, we can protect our information assets, maintain customer trust, and ensure the continued success of our business.