Cybersecurity Policy for Financial Institutions (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the mandatory security requirements for all employees, contractors, vendors, and any other individuals or entities accessing, processing, or storing company information or utilizing company IT assets. This policy applies to all systems, networks, and data within the organization's control, irrespective of location. This policy is designed to protect the confidentiality, integrity, and availability of company data, ensure compliance with applicable laws and regulations, and minimize business disruption caused by cybersecurity incidents. This policy is aligned with Payment Card Industry Data Security Standard (PCI DSS) requirements, commensurate with the organization's low-risk profile, and subject to regular review and updates.

2. Risk Assessment

Given the organization's risk profile, a formal risk assessment will be conducted annually. This assessment will identify potential threats, vulnerabilities, and the likelihood and impact of potential security incidents. While operating in a "low risk environment," the Risk Assessment will focus on the following key areas:

- --Data Security:-- Evaluation of the sensitivity and criticality of company data, with a focus on cardholder data as it relates to PCI DSS compliance.
- --System Security:-- Assessment of the security controls implemented on systems, including network devices, servers, workstations, and mobile devices.
- --Access Control:-- Review of user access rights and permissions to ensure they are aligned with the principle of least privilege.
- --Third-Party Risk:-- Evaluation of the security practices of third-party vendors who have access to company data or systems.

The results of the risk assessment will be used to prioritize security investments and to develop and implement appropriate security controls. The risk assessment methodology and findings will be documented and regularly reviewed by senior management. Mitigation strategies will be implemented to address any identified risks, with prioritized actions for high impact and probable risks.

3. Data Protection

Data protection is paramount. The following measures will be implemented to protect sensitive data:

- --Data Classification:-- All data will be classified based on its sensitivity and criticality. This classification will determine the appropriate level of security controls required to protect the data.
- --Data Encryption:-- Sensitive data, including cardholder data, will be encrypted both in transit and at rest using industry-standard encryption algorithms.
- --Data Masking/Tokenization:-- Where possible, sensitive data will be masked or tokenized to reduce the risk of exposure in the event of a security incident.
- --Secure Data Storage:-- All data will be stored securely, with appropriate physical and logical access controls.

- --Data Retention and Disposal:-- Data will be retained only for as long as it is needed and will be securely disposed of when it is no longer required in accordance with our Data Retention Policy. This includes secure wiping of storage media.
- --Cardholder Data Protection:-- Cardholder data will be protected in accordance with PCI DSS requirements. This includes implementing appropriate access controls, encrypting cardholder data in transit and at rest, and regularly monitoring systems for suspicious activity. Sensitive Authentication Data (SAD) must never be stored.

4. Access Controls

Access to company data and systems will be restricted to authorized personnel only. The following access control measures will be implemented:

- --Principle of Least Privilege:-- Users will be granted only the minimum level of access required to perform their job duties.
- --Strong Passwords:-- All users will be required to use strong passwords that meet minimum complexity requirements. Password policies will be enforced.
- --Multi-Factor Authentication (MFA):-- MFA will be implemented for all users accessing sensitive systems and data, including remote access.
- --Account Management:-- User accounts will be promptly created, modified, and disabled as needed. Regular reviews of user access rights will be conducted to ensure that access remains appropriate.
- --Remote Access:-- All remote access to company networks and systems will be secured using VPNs and MFA. Remote access activities will be logged and monitored.
- --Physical Security:-- Physical access to company facilities and data centers will be restricted to authorized personnel only.

5. Incident Response

A comprehensive Incident Response Plan (IRP) will be maintained and regularly tested to ensure its effectiveness. The IRP will outline the procedures for identifying, containing, eradicating, and recovering from security incidents.

- --Incident Reporting:-- All employees are responsible for reporting suspected security incidents immediately to the designated incident response team.
- --Incident Response Team:-- A dedicated incident response team will be established and trained to handle security incidents.
- --Incident Analysis:-- All security incidents will be thoroughly investigated to determine the root cause and to prevent future occurrences.
- --Incident Communication:-- Clear communication channels will be established to keep stakeholders informed of the status of security incidents.
- --Post-Incident Review:-- A post-incident review will be conducted after each security incident to identify areas for improvement.

6. Security Awareness Training

All employees, contractors, and vendors will be required to participate in annual security awareness training. This training will cover topics such as:

- --Password Security:-- Creating and maintaining strong passwords.

- --Phishing Awareness:-- Recognizing and avoiding phishing attacks.
- --Malware Prevention:-- Protecting against malware infections.
- --Data Security:-- Handling sensitive data securely.
- --Social Engineering:-- Understanding and avoiding social engineering tactics.
- --Incident Reporting:-- Reporting suspected security incidents.

The security awareness training program will be regularly updated to address emerging threats and vulnerabilities. Training completion will be tracked, and refresher training will be provided as needed.

7. Compliance and Auditing

This Cybersecurity Policy is designed to ensure compliance with all applicable laws, regulations, and industry standards, including PCI DSS.

- --Regular Audits:-- Regular internal and external audits will be conducted to assess compliance with this policy and with applicable regulations.
- --Vulnerability Scanning:-- Regular vulnerability scanning will be performed on systems and networks to identify potential security weaknesses.
- --Penetration Testing:-- Periodic penetration testing will be conducted to simulate real-world attacks and to identify vulnerabilities that could be exploited by attackers.
- --Policy Review:-- This Cybersecurity Policy will be reviewed and updated at least annually, or more frequently as needed, to address changes in the threat landscape, business requirements, or regulatory requirements.
- --Documentation:-- All security policies, procedures, and controls will be documented and maintained.
- --PCI DSS Compliance:-- Specific focus on maintaining and demonstrating PCI DSS compliance will be maintained, including but not limited to, annual Self-Assessment Questionnaires (SAQ) and Attestation of Compliance (AOC).

8. Conclusion

This Cybersecurity Policy is critical to protecting company data and systems from cyber threats. All employees, contractors, and vendors 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 or contract. Senior management is committed to supporting and enforcing this policy. This policy will be reviewed annually or more frequently as needed to address evolving threats and business needs. Regular review and adherence to this policy are imperative to maintaining a secure environment and meeting regulatory compliance obligations.