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 defined --"Low-Risk Financial Environment"--, which is characterized by limited customer interaction, predominantly processing ACH transactions (with minimal cardholder data exposure), limited external facing services, and a small, well-managed IT infrastructure. The organization's primary assets consist of internal financial data and operational systems. This policy adheres to relevant regulatory requirements, including elements of the Payment Card Industry Data Security Standard (PCI DSS) applicable to our limited cardholder data scope, and relevant federal regulations. 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, following any significant change to our environment (e.g., new system deployments, significant business process changes), or following a significant security incident, consider factors such as:

- --Asset Criticality:-- The business impact of the compromise of a specific asset. This includes financial loss, reputational damage, legal liabilities, and disruption of critical business operations. We maintain a risk register documenting asset criticality based on a scale of Low, Medium, and High, with corresponding impact assessments.
- --Threat Landscape:-- Potential threats specific to the financial industry and our operational model, including malware (ransomware, banking trojans), phishing attacks targeting financial credentials, social engineering attempts, insider threats (both malicious and unintentional), and Distributed Denial of Service (DDoS) attacks. We subscribe to threat intelligence feeds from reputable sources (e.g., the Financial Services Information Sharing and Analysis Center - FS-ISAC) to stay informed about emerging threats.
- --Vulnerability Analysis:-- Weaknesses in our systems, applications, and processes. This includes regular vulnerability scanning of internal and external systems using tools like Nessus, and periodic penetration testing conducted by qualified third-party vendors. We track vulnerabilities using a defined severity scale (Critical, High, Medium, Low) and prioritize remediation efforts based on severity and asset criticality.
- --Likelihood and Impact:-- The probability of a threat exploiting a vulnerability and the potential business impact. We use a risk matrix to map likelihood and impact, assigning a risk score to each identified risk.

Risk assessment results are documented in a risk register, which includes identified risks, assessed likelihood and impact, proposed mitigation strategies, and assigned

responsibilities. The register is reviewed and updated regularly by the IT Security team and presented to senior management for review and approval. Remediation efforts are prioritized based on the risk score and documented in a remediation plan.

--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). Definitions and examples for each classification are documented in the Data Classification Standard. Appropriate security controls are applied based on classification, as outlined in the Data Security Controls Matrix.
- --Data Encryption:-- Sensitive data, including cardholder data (CHD) covered by PCI DSS (PAN, Expiration Date, CVV) if any, must be encrypted both in transit and at rest. Approved encryption algorithms include:
- --In Transit:-- TLS 1.2 or higher for all web-based communications, SSH for remote access, and IPsec VPN for site-to-site connections.
- --At Rest:-- AES-256 for encrypting databases and files containing sensitive information. Full disk encryption (e.g., BitLocker, FileVault) is required on all laptops and workstations.
- --Data Masking and Tokenization:-- Cardholder data must be masked when displayed (e.g., showing only the last four digits of the PAN) and tokenized when stored or transmitted internally where full card numbers are not required for business purposes, following PCI DSS guidelines. We utilize a PCI-DSS compliant tokenization provider for tokenization services when applicable.
- --Data Retention and Disposal:-- Data retention policies define how long data is stored based on legal, regulatory, and business requirements. These policies are documented in the Data Retention Schedule. Data disposal methods must render the data unrecoverable. Approved methods include:
- --Physical Media:-- Degaussing or physical destruction (shredding).
- --Electronic Media:-- Secure wiping using a software tool that overwrites the data multiple times (e.g., DBAN).
- --Data Loss Prevention (DLP):-- While our environment is low risk, basic DLP measures are implemented to prevent accidental or malicious data leakage. This includes:
- Monitoring outbound email for sensitive keywords and patterns (e.g., credit card numbers, social security numbers) using content filtering rules in our email gateway.
- Implementing endpoint DLP software on workstations to prevent the transfer of sensitive files to USB drives or other removable media.
- Regular audits of file share permissions to ensure that sensitive data is not inadvertently exposed.

--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 are required for accessing sensitive systems and data.
- Multi-factor authentication (MFA) is required for all remote access, administrative accounts, and access to systems containing cardholder data if any, mandated by PCI DSS.
- Password complexity requirements: Passwords must be at least 12 characters long, contain a mix of upper and lowercase letters, numbers, and symbols, and must not be based on personal information or easily guessable patterns. Passwords must be changed every 90 days. Password history is enforced to prevent reuse of previous passwords.
- --Access Control Lists (ACLs):-- Access control lists are used to restrict access to specific files and directories based on user roles and responsibilities. These lists are regularly reviewed and updated as user roles change.
- --Role-Based Access Control (RBAC):-- User access is managed through roles, simplifying administration and ensuring consistent access privileges. Roles are defined based on job function and responsibilities, and access privileges are assigned to each role. Examples include:
- --Finance Clerk:-- Access to accounting software for data entry and reporting.
- --System Administrator:-- Full administrative access to servers and network infrastructure.
- --Database Administrator:-- Access to database servers for maintenance and administration.

Role definitions are documented in the RBAC Matrix.

- --Regular Access Reviews:-- Access privileges are reviewed at least semi-annually to ensure that users have the appropriate level of access. This review includes verifying that users still require the access they have been granted and removing access that is no longer needed. Terminated employees' access is revoked immediately following notification from Human Resources.
- --Privileged Access Management (PAM):-- Access to privileged accounts (e.g., root, administrator) is strictly controlled and monitored. We utilize a PAM solution to manage and audit the use of privileged accounts. Privileged access requires justification and approval through a defined workflow. Session recording is enabled for all privileged sessions.
- --Physical Security:-- Physical access to server rooms, data centers, and other sensitive areas is restricted and monitored. Access is controlled through keycard access systems and surveillance cameras. Visitor access is logged and escorted.

--5. Incident Response--

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

- --Incident Response Plan (IRP):-- 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. The IRP includes specific procedures for different types of incidents, such as malware infections, data breaches, and denial-of-service attacks.
- --Identification:-- Identifying potential security incidents through monitoring logs, security alerts, and employee reports.
- --Containment:-- Isolating affected systems and preventing the incident from spreading.

- --Eradication:-- Removing the root cause of the incident (e.g., removing malware, patching vulnerabilities).
- --Recovery:-- Restoring systems and data to a normal state.
- --Post-Incident Analysis:-- Conducting a thorough analysis of the incident to determine the root cause, identify areas for improvement, and prevent future occurrences.
- --Incident Reporting:-- All employees are responsible for reporting suspected security incidents to the designated security contact (IT Security Manager) or IT department immediately. Reporting channels include phone, email, and a dedicated incident reporting portal.
- --Incident Analysis:-- Security incidents are thoroughly investigated to determine the root cause and prevent future occurrences. Investigations are conducted by the IT Security team, with assistance from other departments as needed.
- --Communication:-- Communication protocols are established to ensure timely and effective communication during a security incident, both internally (to senior management, affected employees) and externally (e.g., to customers, regulatory agencies, law enforcement). The communication plan includes pre-approved templates for communicating with different stakeholders.
- --Regular Testing:-- The incident response plan is tested regularly (at least annually) through tabletop exercises or simulations to ensure its effectiveness. These exercises involve key stakeholders and simulate different types of security incidents. The results of the exercises are used to identify areas for improvement in the IRP.

--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, data protection, and acceptable use of company resources. Training is delivered through online modules and in-person presentations.
- --Phishing Simulations:-- Phishing simulations are conducted at least quarterly to test employees' ability to identify and report phishing attempts. These simulations are designed to mimic real-world phishing attacks and provide employees with immediate feedback on their performance.
- --Regular Updates:-- Security awareness training is updated regularly to address emerging threats and vulnerabilities. Updates are communicated to employees through newsletters, email alerts, and short training modules.
- --Role-Based Training:-- Targeted training is provided to employees with specific security responsibilities (e.g., developers, system administrators, finance personnel). This training covers topics such as secure coding practices, system hardening, and fraud prevention.

--7. Compliance and Auditing--

We maintain compliance with applicable laws, regulations, and industry standards, including PCI DSS elements based on our environment.

- --PCI DSS Compliance:-- We adhere to all applicable PCI DSS requirements for protecting cardholder data if any is processed, including regular vulnerability scanning, penetration testing, and security assessments. We maintain a documented PCI DSS compliance program.
- --Internal Audits:-- Internal audits are conducted at least annually to assess compliance with this Cybersecurity Policy and other security standards. Audits are performed by the internal audit department or a designated internal auditor.
- --External Audits:-- External audits are conducted by qualified security assessors (QSAs) to validate PCI DSS compliance, if applicable.
- --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. The policy update process includes a review by legal counsel and approval by senior management.
- --Documentation:-- Security policies, procedures, and controls are documented and maintained in a central repository. Documentation is regularly reviewed and updated to ensure accuracy and completeness.

--8. Vulnerability Management--

We implement a comprehensive vulnerability management program to identify and remediate security vulnerabilities in our systems and applications.

- --Regular Scanning:-- Automated vulnerability scans are conducted weekly on all internal and external systems using a vulnerability scanner (e.g., Nessus). Scans are configured to identify vulnerabilities based on industry-standard databases (e.g., CVE, CVSS).
- --Patch Management:-- A patch management process is in place to ensure that security patches are applied to systems and applications in a timely manner. Patches are prioritized based on vulnerability severity and asset criticality. Emergency patches are applied immediately.
- --Penetration Testing:-- Penetration testing is conducted at least annually by qualified third-party vendors to identify vulnerabilities that may not be detected by automated scanning. Testing includes both internal and external penetration testing.
- --Remediation Tracking:-- Vulnerabilities identified through scanning and testing are tracked in a vulnerability management system. Remediation efforts are documented and tracked to ensure that vulnerabilities are addressed in a timely manner. Remediation deadlines are based on vulnerability severity and asset criticality, with critical vulnerabilities addressed immediately.

--9. Change Management--

We implement a formal change management process to ensure that changes to systems and applications are properly planned, tested, and implemented to minimize the risk of security incidents.

- --Change Request Process:-- All changes to systems and applications must be submitted through a formal change request process. The change request must include a description of the change, the justification for the change, the potential impact of the change, and the testing plan.
- --Change Approval Board (CAB):-- A Change Approval Board (CAB) reviews and approves all

change requests. The CAB includes representatives from IT, security, and business units.
- --Testing and Validation:-- All changes must be thoroughly tested in a non-production environment before being implemented in production. Testing must include functional testing, security testing, and performance testing.
- --Backout Plan:-- A backout plan must be developed for each change in case the change fails or causes unexpected problems.
- --Documentation:-- All changes must be documented, including the change request, the testing results, and the implementation plan.

--10. Third-Party Risk Management--

We implement a third-party risk management program to assess and mitigate the security risks associated with using third-party vendors and services.

- --Vendor Due Diligence:-- Before engaging a third-party vendor, we conduct due diligence to assess their security posture. This includes reviewing their security policies, certifications (e.g., SOC 2), and security assessment reports.
- --Security Questionnaires:-- We require third-party vendors to complete security questionnaires to provide detailed information about their security controls.
- --Contractual Requirements:-- Our contracts with third-party vendors include specific security requirements, such as data protection requirements, incident reporting requirements, and audit rights.
- --Ongoing Monitoring:-- We monitor third-party vendors on an ongoing basis to ensure that they continue to meet our security requirements. This includes reviewing their security policies, certifications, and security assessment reports, and conducting periodic security audits.
- --Right to Audit:-- We reserve the right to audit third-party vendors to verify their compliance with our security requirements.

--11. 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.