Okay, here's the revised Cybersecurity Policy, incorporating the feedback to address the weaknesses:

Cybersecurity Policy for a Finance Environment

--1. Introduction--

This Cybersecurity Policy outlines the mandatory security measures implemented to protect the confidentiality, integrity, and availability of information assets within our organization. Recognizing the sensitivity of financial data, especially cardholder data (CHD), and the importance of maintaining customer trust and regulatory compliance, this policy is designed to establish and maintain a robust secure operating environment. This policy aligns with industry best practices, and relevant compliance standards, specifically PCI DSS, and other applicable legal and regulatory requirements. All employees, contractors, and third-party vendors are responsible for adhering to this policy. Non-compliance may result in disciplinary action, up to and including termination of employment or contract.

--2. Risk Assessment and Management--

We are committed to ongoing risk management, and regularly assess our environment for threats and vulnerabilities, using a documented risk assessment methodology. Transaction volume is only one factor, and a comprehensive analysis is performed at least annually, or more frequently if there are significant changes to our environment. These assessments consider factors such as:

- --Asset Criticality:-- Classifying data and systems based on their importance to business operations, the potential impact of compromise (e.g., financial, reputational, legal), and the data they hold (e.g., cardholder data, PII). A formal asset inventory is maintained.
- --Threat Landscape:-- Monitoring emerging cyber threats and vulnerabilities specific to the financial sector, our technology stack, and the geographic regions in which we operate. We subscribe to threat intelligence feeds and participate in industry information-sharing groups.
- --Vulnerability Scanning:-- Regularly scanning systems (internal and external) for known vulnerabilities, misconfigurations, and malware. Scans are performed at least quarterly and after significant system changes. Remediation efforts are prioritized based on CVSS scores and potential business impact.
- --Penetration Testing:-- Engaging qualified third-party penetration testers to simulate real-world attacks and identify weaknesses in our security controls. Penetration tests are conducted at least annually and after significant changes to our environment, particularly those affecting cardholder data.
- --Impact Analysis:-- Evaluating the potential impact of security breaches, including financial loss (both direct and indirect), reputational damage, legal and regulatory penalties, business disruption, and loss of customer trust.
- --Risk Treatment:-- Documenting identified risks, assessing their likelihood and impact, and defining appropriate risk treatment strategies (e.g., mitigation, avoidance, transfer, acceptance). All identified risks will be added to a risk register and managed through documented action plans, assigning ownership, timelines and remediation steps.

The results of these risk assessments are documented, presented to senior management, and used to prioritize security controls and inform ongoing security improvements. Mitigation strategies focus on implementing cost-effective controls appropriate for the identified risks, while considering our business objectives and regulatory requirements.

--3. Data Protection--

Protecting sensitive data, especially cardholder data (CHD), 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. Regular reviews are conducted to identify and delete unnecessary data.
- --Data Encryption:-- Encrypting sensitive data at rest and in transit, using strong, NIST-approved encryption algorithms.
- --At Rest:-- AES-256 encryption is required for all sensitive data at rest, including cardholder data, PII, and other confidential information. Key management will be handled using a FIPS 140-2 compliant Hardware Security Module (HSM) or a cloud-based key management service (KMS) with appropriate controls.
- --In Transit:-- TLS 1.2 or higher is required for all data in transit, especially for traffic traversing public networks. Weak cipher suites are prohibited. Internal traffic containing sensitive data must also be encrypted.
- --Data Masking/Tokenization:-- Masking or tokenizing sensitive data when displayed or used in non-production environments (e.g., development, testing). Tokenization is preferred for CHD to reduce the scope of PCI DSS compliance.
- --Data Retention:-- Establishing data retention policies that comply with legal and regulatory requirements, and securely disposing of data when it is no longer needed. Retention periods are defined based on data type, legal obligations, and business needs. Destruction methods must comply with NIST Special Publication 800-88 guidelines for media sanitization. Specifically, CHD should be retained no longer than is strictly necessary to comply with legal, regulatory and business needs.
- --Secure Data Handling:-- Following secure coding practices to prevent vulnerabilities such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities. The OWASP Top Ten is used as a guide for secure coding practices. Static and dynamic application security testing (SAST/DAST) is performed regularly on all internally developed applications.
- --Cardholder Data (CHD) Specific Controls:-- Minimizing the storage of CHD, and ensuring it is protected in accordance with PCI DSS requirements. Regularly monitoring for the presence of unprotected CHD in unexpected locations.

--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 of 12 characters.
- Complexity requirements (uppercase, lowercase, numbers, symbols).

- Regular password changes every 90 days.
- Password history enforced (at least 12 previous passwords remembered).
- Account lockout after a specified number of failed login attempts (e.g., 5 attempts).
- --Multi-Factor Authentication (MFA):-- MFA is required for all remote access, privileged accounts (e.g., administrators, database administrators), and access to systems containing sensitive data, aligned with PCI DSS requirements for strong authentication. Accepted MFA methods include one-time passwords (OTP) generated by an authenticator app, hardware tokens, or biometrics.
- --Authorization:-- Granting users only the access rights necessary to perform their job duties. Access requests are reviewed and approved by a designated data owner or system administrator.
- --Role-Based Access Control (RBAC):-- Assigning access rights based on job roles, simplifying access management and reducing the risk of unauthorized access. Roles are regularly reviewed and updated.
- --Regular Access Reviews:-- Periodically (at least quarterly) reviewing user access rights to ensure they remain appropriate. Access reviews are documented and signed off by the data owner or system owner. Terminated employees' access is revoked immediately upon notification from Human Resources.
- --Privileged Access Management (PAM):-- Implementing a PAM solution to manage and monitor privileged accounts. Privileged sessions are recorded and audited. The use of shared accounts is prohibited.
- --Emergency Access Procedures:-- Establishing documented procedures for granting emergency access to systems and data in situations where normal access controls are insufficient. Emergency access is granted only with appropriate authorization and is subject to audit. All emergency access shall be logged and reviewed as soon as possible after it has been used.
- --Physical Security:-- Implementing physical security controls, such as access badges, surveillance cameras, and locked doors, to protect data centers, server rooms, and other sensitive areas. Physical access logs are regularly reviewed.

--5. Incident Response--

A well-defined and regularly tested incident response plan is essential for effectively handling security incidents. The incident response plan outlines the following and is reviewed and updated at least annually:

- --Incident Response Team (IRT):-- A designated IRT consisting of individuals from various departments (e.g., IT, Security, Legal, Communications). Roles and responsibilities are clearly defined (e.g., Incident Commander, Technical Lead, Communications Lead, Legal Counsel). Contact information for all IRT members is readily available.
- --Incident Detection:-- Monitoring systems for suspicious activity using Security Information and Event Management (SIEM) system, intrusion detection/prevention systems (IDS/IPS), and log analysis. Establishing clear reporting procedures for potential security incidents, including a dedicated email address (security@example.com) and phone number.
- --Incident Containment:-- Isolating affected systems to prevent further damage and spread of the incident. This may involve disconnecting systems from the network, disabling user

accounts, or implementing firewall rules.

- --Incident Eradication:-- Removing the root cause of the incident, such as malware, vulnerabilities, or misconfigurations. This may involve patching systems, removing malicious software, or reconfiguring security settings.
- --Incident Recovery:-- Restoring systems and data to their normal state. This may involve restoring from backups, rebuilding systems, or re-installing applications.
- --Post-Incident Analysis:-- Conducting a thorough post-incident review to identify lessons learned and improve security controls. This review should include a timeline of events, the root cause of the incident, the impact of the incident, and recommendations for preventing similar incidents in the future. A formal incident report is generated and distributed to relevant stakeholders.
- --Communication Protocols:-- Establishing clear communication protocols for notifying relevant stakeholders (e.g., management, employees, customers, law enforcement, regulatory agencies) about security incidents. Communication templates are pre-approved by legal counsel.
- --Escalation Procedures:-- Defining escalation procedures for incidents that require higher-level attention or expertise.
- --Contact Information:-- Maintaining a readily available list of contact information for key personnel, law enforcement, and regulatory agencies.
- --Regular Testing:-- Conducting regular tabletop exercises and simulated attacks to test the effectiveness of the incident response plan.
- --Legal and Regulatory Compliance:-- Ensuring that incident response activities comply with all applicable legal and regulatory requirements, including data breach notification laws and PCI DSS requirements.

--6. Security Awareness Training--

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

- --Phishing Awareness:-- Recognizing and avoiding phishing emails, spear-phishing attacks, and other social engineering tactics. Simulated phishing campaigns are conducted regularly to test employee awareness.
- --Password Security:-- Creating and maintaining strong passwords, using password managers, and avoiding password reuse.
- --Data Handling:-- Protecting sensitive data from unauthorized access, disclosure, or loss. Proper disposal of sensitive data is also covered.
- --Incident Reporting:-- Reporting suspected security incidents promptly and accurately.
- --Policy Compliance:-- Understanding and adhering to this Cybersecurity Policy and other relevant security policies.
- --Physical Security:-- Maintaining awareness of physical security controls and reporting any suspicious activity.
- --Mobile Device Security:-- Securing mobile devices and protecting sensitive data stored on them.
- --Social Media Security:-- Understanding the risks associated with social media and avoiding sharing sensitive information online.

- --PCI DSS Awareness:-- For employees handling cardholder data, specific training on PCI DSS requirements and their responsibilities.

Training is conducted at least annually and reinforced through regular communications, reminders, and security tips. Records of training completion are maintained.

--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, security audits, and annual Self-Assessment Questionnaires (SAQ) or Report on Compliance (ROC) as required by our merchant level.
- --Conduct Internal Audits:-- Regularly conduct internal audits (at least annually) to assess the effectiveness of security controls and identify areas for improvement. Audit findings are documented and remediated.
- --Engage Third-Party Auditors:-- Engage qualified third-party auditors (Qualified Security Assessors - QSAs) to conduct independent security assessments and validate compliance with relevant regulations and standards, including PCI DSS.
- --Document Security Controls:-- Maintain comprehensive documentation of all security controls, policies, procedures, and configurations. Documentation is reviewed and updated regularly.
- --Change Management:-- Implement a formal change management process to ensure that all changes to systems and applications are properly tested, documented, and approved before being implemented in production.

--8. Vendor Management--

We will establish a robust vendor management program to ensure that all third-party vendors who have access to our systems or data maintain appropriate security controls. This includes:

- --Due Diligence:-- Conducting thorough due diligence on all potential vendors, including security assessments, reviews of their security policies and procedures, and background checks.
- --Contractual Agreements:-- Including security requirements in all vendor contracts, such as data protection clauses, incident response requirements, and audit rights.
- --Ongoing Monitoring:-- Regularly monitoring vendor compliance with security requirements, including conducting security audits and reviewing their security reports.
- --Vendor Risk Assessment:-- Vendors will be categorised according to their level of access to sensitive data, and the risk associated with them.

--9. Conclusion--

This Cybersecurity Policy is a living document that will be reviewed and updated regularly (at least annually) to reflect changes in the threat landscape, technology, regulatory requirements, and our business operations. 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, ensure compliance with regulations, and safeguard the continued success of our business.

This revised policy addresses the feedback by:

- --Increasing Specificity:-- Provides more concrete examples and requirements for encryption, data retention, access controls (including MFA and PAM), and other security measures.
- --Strengthening Risk Assessment:-- Emphasizes the need for a robust and documented risk assessment methodology that goes beyond just transaction volume. It also lists key factors to consider during risk assessments and the risk treatment process.
- --Detailing Access Controls:-- Expands the Access Control section to include Privileged Access Management (PAM), emergency access procedures, and more specific password policies.
- --Adding Incident Response Plan Details:-- Includes more detailed information about the incident response team, communication protocols, escalation procedures, and contact information.
- --Adding Vendor Management:-- Ensures vendors meet security requirements.
- --Compliance Focused Updates:-- Ensuring that CHD storage is minimized, regular vulnerability scanning, penetration testing and security audits.
- --Training and Awareness:-- Expanding the scope of training to include more focused elements, such as PCI DSS awareness, mobile device security and social media security.

This revised policy provides a stronger foundation for protecting sensitive data and ensuring compliance with relevant regulations. Remember to customize this policy with your organization's specific information and requirements.