ISMS Framework Development

1. Information Security Policy

1.1 Purpose

The purpose of this Information Security Policy is to ensure the protection of FinM3's information assets against all internal, external, deliberate, or accidental threats. This policy outlines the security standards and principles that must be adhered to by all employees, contractors, and third-party partners.

1.2 Scope

This policy applies to all information systems, data, networks, physical infrastructure, and personnel within FinM3, including all global offices and data centers.

1.3 Policy Statement

FinM3 is committed to ensuring the confidentiality, integrity, and availability of all its information assets. To achieve this, we will:

- Implement appropriate security controls in line with industry best practices and regulatory requirements.
- Regularly assess and manage risks to our information assets.
- Ensure all employees and partners are aware of their security responsibilities through regular training and communication.
- Maintain compliance with applicable laws, regulations, and contractual obligations, including PCI DSS and SOC 2.

1.4 Responsibilities

- **CEO**: Overall responsibility for the Information Security Management System (ISMS).
- **CISO**: Responsible for implementing and maintaining the ISMS and ensuring compliance with this policy.
- **Employees and Contractors**: Responsible for adhering to this policy and reporting security incidents.

1.5 Review and Updates

This policy will be reviewed annually or following any significant security incident, organizational change, or relevant regulatory update.

PCI DSS Section

2.1 Access Control Policy

2.1.1 Purpose

To ensure that only authorized individuals have access to systems and data containing cardholder information, and to enforce the principle of least privilege.

2.1.2 Scope

This policy applies to all employees, contractors, and third-party users who have access to cardholder data or systems that process, store, or transmit cardholder data.

2.1.3 Policy

- **User Access Management**:

    - Access to cardholder data systems is restricted based on job roles and responsibilities.
    - Multi-factor authentication (MFA) is required for accessing cardholder data environments.
    - Regular reviews of user access rights will be conducted to ensure ongoing compliance.
    - Temporary access for specific projects or audits will be time-bound and monitored.
- **Password Management**:
    - Passwords must be complex and changed every 90 days.
    - Passwords must not be reused for a period of 12 months.
    - Accounts are locked after five unsuccessful login attempts and require manual intervention for reactivation.
- **Remote Access**:
    - Remote access to cardholder data systems is restricted to authorized personnel using a secure VPN with MFA.

2.1.4 Monitoring and Enforcement

- Access logs will be monitored and reviewed daily for any unauthorized access attempts.
- Violations of this policy will be subject to disciplinary action.

2.2 Data Encryption Policy

2.2.1 Purpose

To protect cardholder data and other sensitive information through encryption, ensuring that data is secure both at rest and in transit.

2.2.2 Scope

This policy applies to all cardholder data processed, stored, or transmitted by FinM3, including data in databases, file systems, and across networks.

2.2.3 Policy

- **Encryption Standards**:
  - All cardholder data must be encrypted using AES-256 or an equivalent or stronger encryption algorithm.
  - Encryption keys must be stored securely, with access restricted to authorized personnel only.
- **Data at Rest**:
  - Cardholder data stored in databases, file systems, or any other storage medium must be encrypted at rest.
  - File systems containing sensitive data must be encrypted using full-disk encryption technologies.
- **Data in Transit**:
  - Cardholder data must be encrypted during transmission over any network using TLS 1.2 or higher.
  - Email transmission of cardholder data is prohibited unless the data is encrypted end-to-end.

2.2.4 Key Management

- Encryption keys must be rotated annually or after any suspected compromise.
- Access to encryption keys is restricted and must be audited regularly.

2.3 Monitoring and Logging

2.3.1 Purpose

To ensure that all access to cardholder data and critical systems is logged, monitored, and retained for incident response and forensic analysis.

2.3.2 Scope

This policy applies to all systems within the cardholder data environment (CDE) and any system that interfaces with it.

2.3.3 Policy

- **Logging**:
    - All access to cardholder data, system components, and administrative functions must be logged.
    - Logs must include user ID, date and time, event type, and data accessed.
- **Monitoring**:
    - Real-time monitoring systems must be in place to detect unauthorized access attempts, policy violations, and anomalous activity.
    - Alerts must be configured for critical events such as failed login attempts, unauthorized access, and changes to system configurations.
- **Log Retention**:
    - Logs must be retained for a minimum of one year, with at least three months of logs readily accessible for review.

2.3.4 Review and Response

- Logs must be reviewed daily by the IT security team.

- Any identified anomalies or incidents must be escalated according to the Incident Response Plan.

2.4 Incident Response Plan

2.4.1 Purpose
To establish a structured and effective process for identifying, responding to, and mitigating security incidents, particularly those involving cardholder data.

2.4.2 Scope
This plan applies to all security incidents that may affect the confidentiality, integrity, or availability of cardholder data or other critical information systems.

2.4.3 Incident Response Team (IRT)
- **Members**:
    - CISO (Incident Commander)
    - IT Security Manager
    - Legal and Compliance Officer
    - Communications Manager
    - Relevant IT and business unit representatives

2.4.4 Incident Classification
- Incidents will be classified according to severity, with categories ranging from low to critical based on the potential impact on cardholder data and operations.

2.4.5 Response Procedures
- **Detection**: Use automated monitoring tools to detect potential security incidents.

- **Containment**: Immediately isolate affected systems to prevent further damage or data loss.
- **Eradication**: Remove the root cause of the incident, such as malware or unauthorized access.
- **Recovery**: Restore affected systems and data to a secure state.
- **Communication**: Notify stakeholders, including customers and regulatory bodies, as required.
- **Post-Incident Review**: Conduct a detailed review to identify lessons learned and improve future responses.

2.4.6 Documentation and Reporting

- All incidents must be documented in the Incident Log.
- A formal incident report must be completed within 48 hours of the incident being resolved.

SOC 2 Section

3.1 Change Management Policy

3.1.1 Purpose

To ensure that all changes to information systems are managed in a controlled manner, reducing the risk of unintended disruptions or vulnerabilities.

3.1.2 Scope

This policy applies to all changes to systems, applications, and infrastructure within FinM3 that could affect the security, availability, confidentiality, or privacy of customer data.

3.1.3 Policy

- **Change Request**:
    - All changes must be documented in a Change Request (CR) form that includes the rationale, impact analysis, and rollback procedures.
    - Emergency changes must be documented within 24 hours of implementation.
- **Approval Process**:
    - All CRs must be reviewed and approved by the Change Advisory Board (CAB), which includes representatives from IT, security, and business units.
    - High-risk changes require additional approval from the CISO.
- **Testing and Validation**:
    - All changes must be tested in a controlled environment before deployment.
    - Affected systems must be validated post-deployment to ensure changes have been applied correctly.
- **Rollback Plan**:
    - Every change must have a documented rollback plan to restore systems to their previous state in case of issues.

3.1.4 Monitoring and Reporting

- All changes will be logged and monitored for any unexpected impact on systems and data.
- A monthly report of all changes will be reviewed by the CAB.

3.2 Third-Party Management

3.2.1 Purpose

To ensure that all third-party vendors handling FinM3's data comply with security standards and do not introduce vulnerabilities to the environment.

3.2.2 Scope

This policy applies to all third-party vendors, service providers, and partners that have access to FinM3's data or systems.

3.2.3 Policy

- **Vendor Assessment**:
    - All vendors must undergo a security assessment before engagement to evaluate their controls, particularly around data protection.
    - Critical vendors must provide evidence of compliance with SOC 2 or equivalent standards.
- **Contractual Obligations**:
    - Contracts with vendors must include clauses requiring adherence to FinM3's security policies, including data encryption, access controls, and incident reporting.
    - Vendors must notify FinM3 of any security incident within 24 hours.
- **Ongoing Monitoring**:
    - Annual reviews of vendors' security controls must be conducted, with more frequent reviews for high-risk vendors.
    - A formal review of vendor performance and security posture must be completed annually.