Information Security Management System (ISMS) Policy Statement

1. Introduction

First City Monument Bank (FCMB) is committed to protecting the confidentiality, integrity, and availability of its information assets. This ISMS policy outlines our approach to managing information security risks and ensuring compliance with regulatory requirements.

2. Scope and Applicability

This policy applies to all FCMB employees, contractors, vendors, and third-party service providers. It covers all information assets, including customer data, financial information, and sensitive business data.

3. Information Security Objectives

The bank's information security objectives cover:

a. Protect customer data and maintain confidentiality.
b. Ensure integrity of financial information and business data.
c. Maintain availability of information systems and services.
d. Comply with regulatory requirements and industry standards.
e. Continuously improve information security practices.

4. Risk Management

a. Conduct regular risk assessments using ISO 27001:2022 risk assessment methodology.
b. Identify, assess, and prioritize information security risks.
c. Implement risk treatment plans and controls.
d. Review and update risk assessments annually or as needed.

5. Information Security Controls

a. Access Control: Implement role-based access controls, multi-factor authentication, and secure password policies.
b. Network Security: Utilize firewalls, intrusion detection/prevention systems, and encryption.
c. Data Protection: Implement data encryption, backups, and secure data disposal.

d. Incident Response: Establish incident response plan and procedures.

e. Business Continuity: Develop business continuity plans and conduct regular testing.

6. Compliance and Accountability

a. Adhere to the Nigeria Data Protection Act (2023), Cybercrime Prohibition Act (2015), and other relevant regulations.

b. Ensure compliance with ISO 27001:2022 standards.

c. Employees, contractors, and vendors must comply with this policy.

d. Breaches may result in disciplinary action, contract termination, or legal consequences.

7. ISMS Governance

a. Designate Information Security Officer (ISO) to oversee ISMS governance.

b. Establish ISMS governance structure and roles.

c. Conduct regular ISMS reviews and updates.

8. Data Protection

a. Implement data protection by design and default.

b. Conduct data protection impact assessments.

c. Ensure data subject rights.

9. Training and Awareness

a. Provide regular information security training for employees.

b. Conduct security awareness programs.

c. Ensure employees understand information security responsibilities.

10. Continuous Monitoring and Improvement

a. Conduct regular security audits and reviews.

b. Monitor ISMS performance using key performance indicators (KPIs).

c. Continuously improve information security practices.