1.0 Policy Statement

At Sterling Bank Limited, we recognize that information and information systems are critical assets, essential to maintaining trust, ensuring compliance, and achieving our business objectives. Protecting the confidentiality, integrity, and availability of these assets is central to our operations and long-term success.

In addition, the Bank recognizes its role as a critical component of Nigeria's financial services infrastructure and the broader national critical information infrastructure. Accordingly, cybersecurity practices are aligned to support the resilience, stability, and secure interconnectivity of the financial ecosystem and its dependencies.

In line with ISO/IEC 27001, Sterling Bank is committed to:

- Establishing and maintaining an information security management system (ISMS) that is appropriate to the Bank's purpose and aligned with its strategic objectives.
- Meeting all applicable legal, regulatory, contractual, and stakeholder requirements related to information security.
- Continually improving the ISMS to adapt to changing risks, business needs, and the evolving threat landscape.

To achieve these commitments, Sterling Bank shall pursue the following information security objectives:

1. Ensure secure, resilient, and trusted digital and customer channels by protecting customer data, securing customer platforms against downtime due to cyber incidents to maintain high availability of customer-facing services.
2. Improve operational efficiency and reduce risk by automating security processes, optimizing security tools and services, and embedding security seamlessly into business operations.
3. Protect the confidentiality, integrity, and availability of data and technology platforms by embedding security controls across systems, data lifecycle, and automated processes.
4. Ensure secure deployment and operation of distributed and alternative infrastructure through applicable physical, environmental, and network security controls.

5. Protect revenue, financial systems, and customer assets by minimizing losses from cyber incidents, fraud, and service disruptions while ensuring the security of core banking operations.
6. Optimize cybersecurity investment and service delivery through risk-based prioritization and efficient utilization of resources while maintaining effective control coverage.
7. Maintain strong cybersecurity governance, effective risk management, and full regulatory compliance through alignment with applicable standards, timely reporting, and enforcement of controls.

To support these objectives, Sterling Bank shall implement suitable policies, processes, procedures, organizational structures, and technical and physical controls. We will also provide regular awareness and training to employees and stakeholders to promote a culture of information security and resilience.

This policy shall be maintained as documented information, communicated to all employees, contractors, and third parties, and made available to interested parties as appropriate. It will be reviewed annually—or sooner if required—to ensure continued suitability, adequacy, and effectiveness.