INFORMATION & CYBERSECURITY POLICY STATEMENT

- The Board and Management of First Bank of Nigeria Ltd located at 35 Marina, Lagos Nigeria, which operates in the financial sector, are committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout the organization in order to preserve its competitive edge, assets, profitability, legal, regulatory as well as contractual, compliance and commercial image. Information and cyber security requirements will continue to be aligned with organizational goals, and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, electronic operations, e-commerce and reducing information and cyber security risks to acceptable levels.
- FirstBank's ISMS shall comply with the ISO 27001 Information Security standard, PCIDSS (Payment Card Industry Data Security Standard), and applicable regulatory and legal requirements related to cybersecurity and privacy.
- FirstBank's current strategy and Information & Cyber Security Risk framework provides the context for identifying, assessing, evaluating, and controlling information & cyber security risks through the establishment and maintenance of an ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information & cyber security risks are controlled. The Chief Risk Officer is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.
- In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems, and information & cyber security incident management are fundamental to this policy. All employees of FirstBank have the responsibility of reporting Security breaches.
- All employees of First Bank of Nigeria Ltd and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All staff and certain external parties will receive or be required to provide appropriate training.
- FirstBank is committed to setting measurable information security objectives aligned with this policy. The framework for establishing, reviewing, and updating these objectives is documented in the ISMS Manual.
- FirstBank shall regularly review and update cybersecurity risk management policies and practices to align with industry standards and emerging threats.
- Support transparent communication with the board on the level of technology and cyber risk, to enable business-oriented decisions on investments and priorities.
- The ISMS is subject to continuous and systematic review with improvements, where necessary.
- FirstBank has established Risk Committees with members drawn from across the Bank.
- The Chief Information Security Officer is responsible for implementing and overseeing the Bank's Information and cyber security programme and strategy and mitigating information and cyber security risks.
- The Chief Risk Officer has ultimate responsibility for maintaining compliance to PCI DSS and ISO 27001 standards.

- The Chief Risk Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed and reapproved by the Board at least annually and also in the event of relevant changes and/or incidents
- A current version of this document is available to all members of staff on the corporate intranet.