# Information Security Policy

Access Bank (SL) Limited is committed to protecting the security, confidentiality, and integrity of all information regardless of format or storage medium in accordance with applicable laws, regulations, and industry standards. Information is recognized as a critical business asset that supports our service delivery, customer trust, and operational continuity.

Information security at Access Bank is viewed as a key enabler of our business strategy and is essential for achieving long-term organizational goals.

To this end, the Bank's management is committed to ensuring that:

- All information security policies, procedures, and guidelines are developed and managed centrally by the Information Security team, under the leadership of the Information and Cyber Security Unit and aligned with the bank-wide governance framework.
- All employees, third-party service providers, and contractors undergo periodic information security training to raise awareness and build competence in protecting the Bank's information assets.
- The Bank complies with all applicable legal, regulatory, and contractual requirements, including but not limited to the Bank of Sierra Leone directives, PCI DSS, and the ISO/IEC 27001:2022 standard.
- Information Security Management System (ISMS) objectives are defined, tracked, and resourced appropriately to ensure they are met effectively.
- Continual improvement is embedded into the ISMS through regular monitoring, internal audits, management reviews, incident analysis, and stakeholder feedback.
- This Information Security Policy and associated controls are reviewed at least once a year or following any major changes, to ensure continued relevance, adequacy, and effectiveness.

# Information Security Objectives

- Ensure 100% protection of critical information assets by performing quarterly risk assessments and implementing required controls to prevent unauthorized access, data breaches, and cyber threats.
- Maintain 99.9% uptime of critical banking services and customer-facing platforms annually, reducing revenue loss and improving service continuity.
- Achieve and sustain 99% confidentiality, integrity, and availability (CIA) of critical systems and data by enforcing access control, data classification, and patch management as part of the annual ISMS plan.
- Achieve 100% annual compliance with all applicable regulatory, legal, and contractual obligations, including directives from the Bank of Sierra Leone, PCI DSS, and ISO/IEC 27001 standards.
- Deliver annual ISMS awareness and role-based security training to at least 90% of staff and key third-party personnel, increasing competence and reducing human-related risks.
- Conduct 100% internal ISMS audits and at least one annual external audit to monitor the effectiveness of security controls and drive continual improvement.