Access Bank Kenya - Integrated Management System Policy Statement

At Access Bank Kenya, we recognise the critical importance of **ensuring the continuity of our business operations, especially during times of unforeseen disruptions or crises**. As such, we are committed to establishing, implementing, maintaining, and continually improving a robust Business Continuity Management System (BCMS) in accordance with the requirement of ISO 22301:2019. Our commitments are Resilience, Preparedness, Leadership, Compliance, Communication, Training, and Awareness, Testing and Exercises and Continual Improvement in line with our documented Business Continuity Management System Policy.

Access Bank Kenya is committed to improving its information security posture by **Preserving the Availability, Confidentiality, and Integrity of the Bank's Information assets** (this includes physical and electronic information, cardholder data, etc.) throughout the organization to preserve its competitive edge, assets, profitability, legal, regulatory as well as contractual, compliance and commercial image. As such, we are committed to establishing, implementing, maintaining, and continually improving a robust Information Security Management System (ISMS) in accordance with the requirement of ISO 27001:2022. Our commitments are deploying technical security controls on the Bank's infrastructure, Security and Incident Monitoring, Leadership, Compliance, Communication, Training, and Awareness, and Continual Improvement in line with our documented Information Security Management System Policy.

Access Bank Kenya has implemented and is certified to best practice standards and frameworks which include ISO 22301 (Business Continuity Management System), and ISO 27001 (Information Security Management System). The implementation was conducted by harmonising all activities together, which resulted in the Integrated Management System (IMS).

Management has outlined the following objectives for the Integrated Management System which the Bank is certified to:

- Objective 1 – Protect 100% of customers' confidential information, as well as the integrity, and availability of Access Bank (Kenya) Plc.'s Information assets.

- Objective 2 - Improve information security and business continuity awareness culture across the bank by 100%.

- Objective 3 – Recover and restore all critical business processes within 95% assurance of the target business recovery objectives.

- Objective 4 - Ensure 100% adherence to regulatory and legal requirements that pertain to Information security and business continuity, annually.

To achieve the Information Security objectives, Access Bank Kenya has established Information Security Policies which comprise:

- Network Access Policy
- Physical Access & Environmental Policy
- System Operations and Administration Policy
- System Acquisition, Development, and Maintenance Policy
- E-mail Usage
- Internet Usage
- Malicious Code
- E-Business Policy
- Reporting Information Security Incident
- Change Management
- Configuration Management
- Data Protection and Privacy
- Acceptable Use Policy
- Logical Access Control
- Business Continuity
- HR Admin Security
- Mobile Device
- Clear Desk and Clear Screen Policy
- Cryptography
- Service Accounts

Access Bank Kenya's Executive leadership is committed to proactively:

1. Implement the necessary capabilities to ensure the continuity of its critical business functions in the event of a major disruption or disaster, and to ensure the recovery of those critical functions to an operational state within an acceptable timeframe.
2. Ensure that Integrated Management System (IMS) objectives are set and that adequate resources are allocated to achieve them. The IMS objectives shall be consistent with business requirements and compatible with the strategic direction of the Bank.
3. Obtain ideas for improvement through regular meetings with customers and stakeholders.
4. Raise the awareness of all employees and stakeholders to ensure that the benefits of achieving the IMS objectives are understood.
5. Ensure that all employees are made aware of and understand the IMS policy, procedures and supporting documentation through training and the provision of information. Compliance will be confirmed because of formal internal audits and management reviews, which will be conducted at least annually.
6. Continually improve the effectiveness of the IMS across all areas within scope.

7. Enhance current processes to bring them into line with good practice as defined within ISO 27001 and ISO 22301.
8. Achieve certification to the Information Security Management System, and Business Continuity Management System and maintain them on an ongoing basis.
9. Increase the level of proactivity (and the stakeholder perception of proactivity) about the ongoing management of the IMS.
10. Make processes and controls more measurable to provide a sound basis for informed decisions.

This policy is publicly available to all interested parties and is reviewed periodically to account for applicable local, statutory, regulatory, and customer requirements and any changes in business activity.

This Policy applies to all Bank employees, its contractors, its consultants, and other individuals affiliated with Third Parties who have access to the Bank's information or business interests.

Thank you.

Samuel Addae Minta
Country Managing Director, Access Bank Kenya