INFORMATION SECURITY POLICY STATEMENT

Access Bank Botswana is committed to improving its information security posture, and the resilience of its operations in the face of unforeseen events and disruptions, as well as ensuring the optimum delivery of financial services.

As part of its continued growth strategy, Access Bank is focused on mainstreaming sustainable business practices into its operations. We are also committed to the effective implementation, maintenance, and continual improvement of the information security management system to support the achievement of our business goals.

To achieve the Information Security objectives, Access Bank Botswana has established an Information Security Policy which comprises:

- Access Bank Botswana Cyber Incidence Response
- 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
- USSD Usage
- Cryptography
- Service Accounts

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

- 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.

- 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.
- Obtain ideas for improvement through regular meetings with customers and stakeholders.
- Raise the awareness of all employees and stakeholders to ensure that the benefits of achieving the ISMS objectives are understood.
- 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.
- Continually improve the effectiveness of the ISMS across all areas within scope.
- Enhance current processes to bring them into line with good practice as defined within ISO 27001.
- Achieve certification to the Information Security Management System and maintain them on an ongoing basis.
- Increase the level of proactivity (and the stakeholder perception of proactivity) about the ongoing management of the ISMS.
- 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 take account of 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.
Sheperd Aisam
Managing Director, Access Bank Botswana