

Access Bank (Rwanda) Plc – Information Security and Business Continuity Policy and Objectives Statement

At Access Bank (Rwanda) Plc, we recognise the critical importance of **ensuring the continuity of our business operations, especially during times of unforeseen disruptions or crises**. We also prioritise the protection of our information to remain a well-known, reputable Bank.

Access Bank (Rwanda) Plc has implemented best practice standards and frameworks, which include ISO 22301:2019 (Business Continuity Management System ‘BCMS’) and ISO 27001:2022 (Information Security Management System ‘ISMS’). The implementation was conducted by harmonising all activities together, which resulted in the **Integrated Management System (IMS)**.

The Bank is set to achieve the following objectives:

- **Objective 1:** Protect 100% of customers’ confidential information, as well as the integrity and availability of Access Bank (Rwanda) Plc.’s Information assets.
- **Objective 2:** Provide assurance of information systems resilience
- **Objective 3:** Improve information security and business continuity awareness culture across the bank by 100%
- **Objective 4:** Recover and restore all critical business processes within 95% assurance of all the target business recovery objectives
- **Objective 5:** Containment of financial impact
- **Objective 6:** Maintain a continuous improvement of its capacity to meet the customers’ increasing and dynamic banking needs
- **Objective 7:** Protection of the bank’s reputation

To achieve the Information Security and Business Continuity objectives, Access Bank Rwanda has established the following policies:

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

These policies are available upon request.

Access Bank Rwanda’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 the Information Security and Business Continuity objectives are set and that adequate resources are allocated to achieve them. The 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 Information Security and Business Continuity 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 statement 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 statement 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.

We adhere you to take all necessary security measures when doing business with Access Bank (Rwanda) Plc.

Thank you.

Faustin R. Byishimo
Country Managing Director

19th , September, 2025
Date