Information Security and Business Continuity Policy

Our Vision is to be the World's Most Respected African Bank.

As Managing Director, I am committed to the continuous improvement of Information Security controls and culture throughout the business. We will work as one team to effectively secure our IT systems and information by:

1. Controlling access through the implementation of user names, passwords and system privileges.

2. Making sure that security is an integral part of information systems including segregation of duties, change control procedures and agreed testing and approval processes.

3. Ensuring Information Security events and weaknesses are formally managed to allow timely corrective action to be taken.

4. Protecting critical information systems from the effects of major failures or disasters by deploying appropriate resilient infrastructure.

5. Ensuring redundant equipment, media and papers are disposed of securely.

6. Making sure information is protected to an appropriate level, based upon the impact of its disclosure, modification, or loss

7. Complying with all relevant information management legislation, regulations, and standards.

8. Making sure that employees are clear about their responsibilities regarding ownership of information security, and that we expect them to take their legal and moral role seriously.

9. Managing the security of all computer systems and supporting infrastructure through the implementation of appropriate technical security controls.

10. Access Bank is committed to aligning its processes and operations to the IS027001 22301 standard and PCIDSS requirements.

We will annually review the Information Security policy and the way it operates, or frequently in the case of significant change to the nature or scope of risk in the business.

Signed by

Ganiyu Sanni,
Managing Director

☎ **+23276926032**
Access Bank (SL) Limited

access

more than banking