BBC BANK UGANDA LIMITED

Plot 14, Kampala Road, P.O. Box 70421, Kampala

ICT POLICY MANUAL

Version 6.0

August 2021

Document Control

Item	Detail
Document type	Policy
Policy owner	Head of Information and Communication Technology
Effective date	1 September 2021
Review frequency	Every two (2) years or upon significant change
Next review due	August 2023
Classification	Internal

Approvals

Role	Name	Signature	Date
Head of ICT	Robert Ssebaggala	Signed	16/08/2021
Managing Director	Dr. Catherine Nalwoga	Signed	20/08/2021
Chairperson, Board Audit and Risk Committee			
Chairperson, Board of Directors			
Company Secretary			

Revision history

Version	Date	Description	Owner
1.0	14/03/2011	Initial ICT policy	Head IT
2.0	02/05/2013	Review	Head IT
3.0	21/07/2015	Review; added e-mail use	Head IT
4.0	18/09/2017	Finacle 10 migration update	Head ICT
5.0	11/06/2019	Review	Head ICT
6.0	16/08/2021	Review; remote working added	Head ICT

1. Purpose and Scope

This policy sets out the principles for the acquisition, management, use and protection of information and communication technology (ICT) resources of BBC Bank Uganda Limited ("the Bank"). It applies to all employees, contractors, consultants, temporary staff and third parties who access the Bank's information systems, including the core banking system, ATM switch, internet banking, mobile banking and supporting infrastructure.

The policy is aligned to the Bank's Strategic Plan 2021–2025, the Financial Institutions Act 2004 (as amended) and the Bank of Uganda Risk Management Guidelines.

2. ICT Governance

2.1 Roles and responsibilities

- The Board of Directors is responsible for approving the ICT policy and ICT strategy and for oversight of ICT risk through the Board Audit and Risk Committee.
- The ICT Steering Committee (ITSC), chaired by the Managing Director, shall meet at least quarterly to prioritise ICT investments, monitor projects and review ICT risk. Minutes shall be kept by the Head of ICT.
- The Head of ICT is responsible for day-to-day management of ICT resources and implementation of this policy.
- The ICT Security Officer shall report to the Head of ICT and is responsible for user administration, security monitoring and awareness.
- Internal Audit shall carry out periodic independent reviews of ICT controls.

2.2 ICT strategy

The Head of ICT shall maintain an ICT strategy aligned to the Bank's strategic plan, reviewed annually by the ITSC and approved by the Board.

3. Logical Access Control

3.4 User access management

- Access to any system shall be granted only on the basis of a completed and signed User Access Request Form approved by the Head of Department before the account is created.
- Access rights shall be restricted to those required for the user's job (least privilege).
- Transfers (movers) shall be notified by Human Resources and previous access removed within five (5) working days of the transfer.
- Human Resources shall notify ICT of all exits on or before the last working day. ICT shall revoke all access within twenty-four (24) hours of notification. (Clause 3.4(q))
- User access reviews for the core banking system shall be performed semi-annually by Heads of Department and evidenced.
- Accounts not used for ninety (90) days shall be disabled.

3.5 Identity and generic accounts

- Each user shall have a unique user ID. Generic or shared user IDs are prohibited, except for system service accounts approved by the Head of ICT and recorded in the Service Account Register.
- Default and built-in administrator accounts shall be renamed and their use restricted and logged.
- Vendor and third-party accounts shall be enabled only for the duration of an approved support task and disabled immediately afterwards.

3.6 Password policy

All systems shall enforce the following minimum password standards:

Parameter	Requirement
Minimum length	8 characters
Complexity	Upper case, lower case, digit and special character
Maximum password age	30 days for user accounts
Password history	Last 12 passwords may not be reused
Account lockout	After 3 consecutive failed attempts
Lockout duration	Until reset by ICT Service Desk
Screen lock	After 15 minutes of inactivity
Password never expires	Permitted only for approved service accounts
Multi-factor authentication	Required for privileged users and remote access

4. Change Management

- All changes to production systems shall be raised as a Change Request (CR) and approved by the Change Advisory Board (CAB) before implementation.
- Business users shall sign off User Acceptance Testing (UAT) before a change is deployed.
- Developers shall not have access to deploy to production. Deployments shall be performed by ICT Operations.
- Emergency changes may be implemented with the verbal approval of the Head of ICT and shall be approved retrospectively by CAB within two (2) working days.
- Every change shall have a documented backout plan.

5. Data Backup

- Critical databases shall be backed up daily (incremental) and weekly (full).
- Weekly full backup tapes shall be transferred to the Disaster Recovery site within 48 hours and recorded in the tape movement register.
- Backup failures shall be logged as incidents and resolved within 24 hours.
- Restore tests shall be performed at least quarterly for each critical system and signed off by the Head of ICT.

6. Business Continuity and Disaster Recovery

- The Bank shall maintain an ICT Disaster Recovery Plan (DRP) covering all critical systems, reviewed annually.
- The DRP shall be tested at least once a year and test results reported to the ITSC and the Board Audit and Risk Committee.

7. Third-Party and Outsourcing

- All ICT service providers shall sign a contract, service level agreement and non-disclosure agreement.
- Remote access by vendors shall be via approved VPN, time-bound and monitored.

8. Logging and Monitoring

- Security and audit logs of critical systems shall be retained for at least twelve (12) months and reviewed regularly by the ICT Security Officer.

9. Acceptable Use, E-mail and Internet

Users shall use ICT resources for official purposes. Personal use shall be minimal and shall not interfere with work. Users shall not install unlicensed software or connect personal devices to the Bank network without approval.

10. Enforcement

Breach of this policy may result in disciplinary action in accordance with the Bank's Human Resources Manual.

~ End of Policy ~