baobab

Information Security Management System Policy

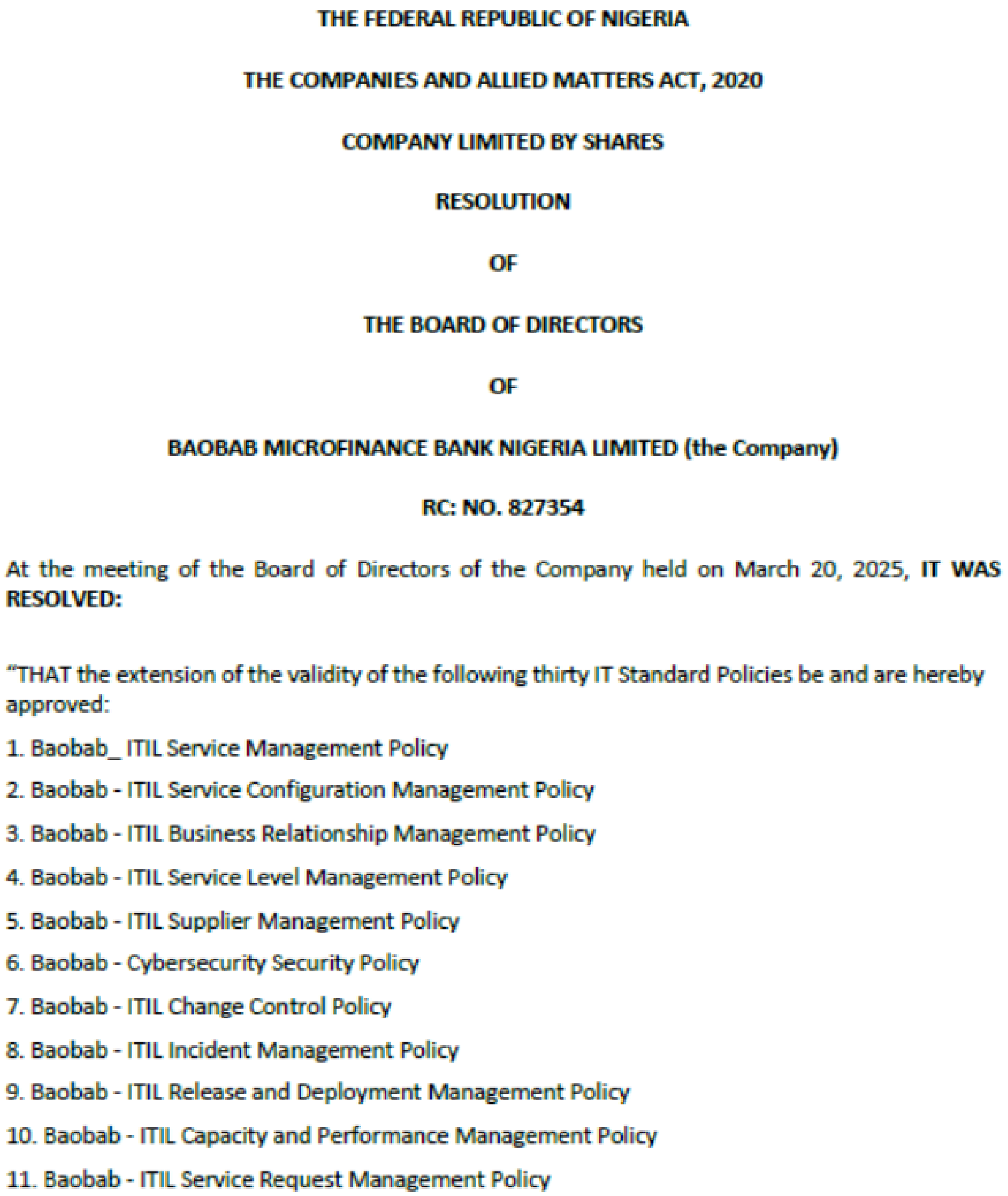
February 2025

This details the bank's commitment to protecting information resources, achieving ISO/IEC 27001 certification, and ensuring compliance with regulatory requirements.

Key aspects include defining the scope of the ISMS, emphasising the importance of information security, outlining policy statements and objectives, assigning roles and responsibilities, and establishing procedures for risk management, auditing, and documentation.

The policy also addresses continual improvement and focuses on maintaining the confidentiality, integrity, and availability of information.

Issuer	*Information Security*
Type	*Policy*
Reference	*SMS-PCY-A05007*
Version	*V 2.0*
Status	*Approved*
Scope	*Information Security Management Policy*
Author	*Ahmed Adewuyi*
Validator	*Babatunde Baruwa*
Date of the previous draft	*Feb, 2023*
Date of validation by the Executive Committee	*15/03/2025*
Date of effect	*20/03/2025*
Date Reviewed	*26/02/2025*
Next Review Date	*27/02/2027*
Document Classification	*Restricted / Internal*



THE FEDERAL REPUBLIC OF NIGERIA

THE COMPANIES AND ALLIED MATTERS ACT, 2020

COMPANY LIMITED BY SHARES

RESOLUTION

OF

THE BOARD OF DIRECTORS

OF

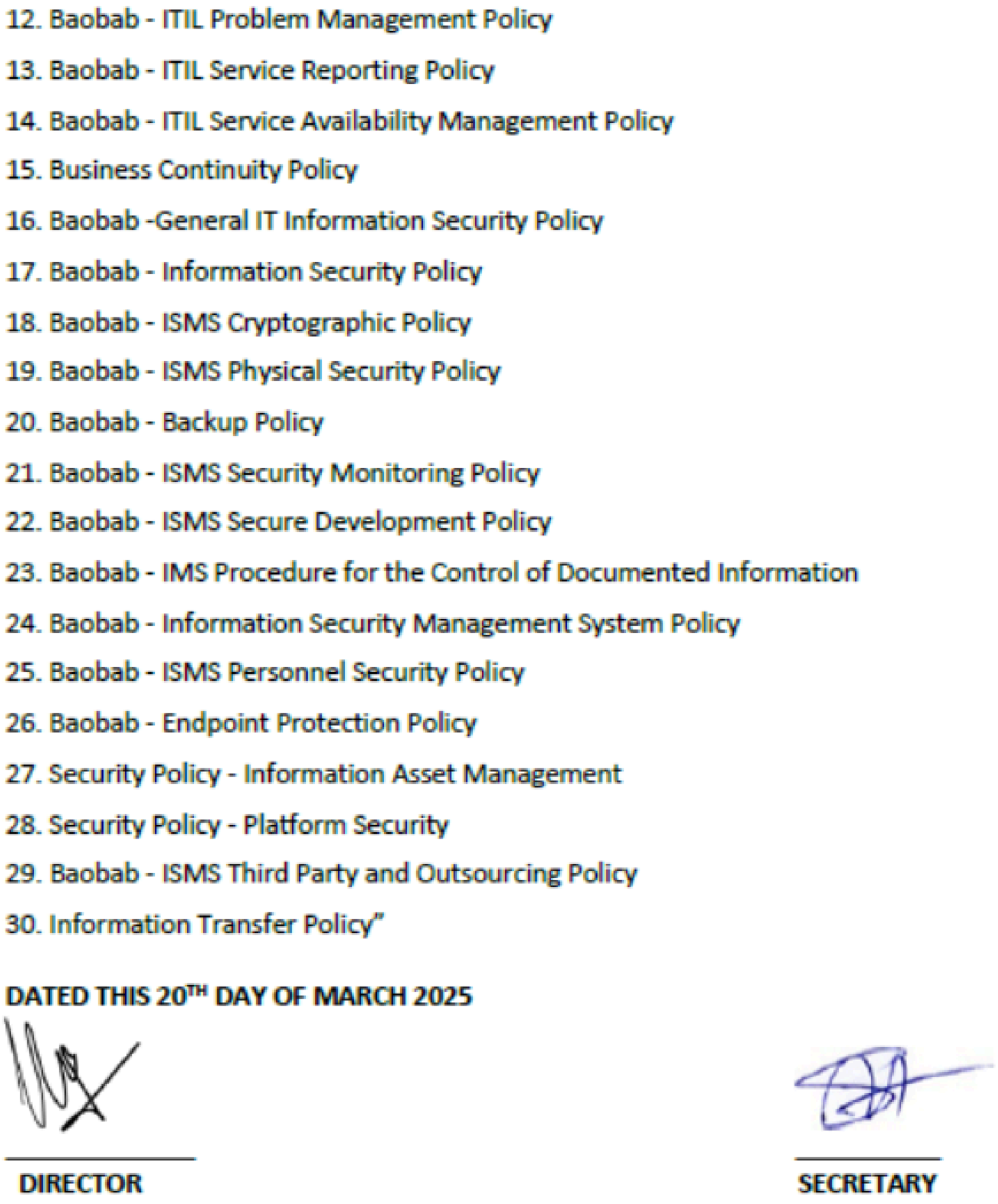
BAOBAB MICROFINANCE BANK NIGERIA LIMITED (the Company)

RC: NO. 827354

At the meeting of the Board of Directors of the Company held on March 20, 2025, **IT WAS RESOLVED:**

"THAT the extension of the validity of the following thirty IT Standard Policies be and are hereby approved:

1. Baobab_ ITIL Service Management Policy
2. Baobab - ITIL Service Configuration Management Policy
3. Baobab - ITIL Business Relationship Management Policy
4. Baobab - ITIL Service Level Management Policy
5. Baobab - ITIL Supplier Management Policy
6. Baobab - Cybersecurity Security Policy
7. Baobab - ITIL Change Control Policy
8. Baobab - ITIL Incident Management Policy
9. Baobab - ITIL Release and Deployment Management Policy
10. Baobab - ITIL Capacity and Performance Management Policy
11. Baobab - ITIL Service Request Management Policy



12. Baobab - ITIL Problem Management Policy
13. Baobab - ITIL Service Reporting Policy
14. Baobab - ITIL Service Availability Management Policy
15. Business Continuity Policy
16. Baobab -General IT Information Security Policy
17. Baobab - Information Security Policy
18. Baobab - ISMS Cryptographic Policy
19. Baobab - ISMS Physical Security Policy
20. Baobab - Backup Policy
21. Baobab - ISMS Security Monitoring Policy
22. Baobab - ISMS Secure Development Policy
23. Baobab - IMS Procedure for the Control of Documented Information
24. Baobab - Information Security Management System Policy
25. Baobab - ISMS Personnel Security Policy
26. Baobab - Endpoint Protection Policy
27. Security Policy - Information Asset Management
28. Security Policy - Platform Security
29. Baobab - ISMS Third Party and Outsourcing Policy
30. Information Transfer Policy"

DATED THIS 20TH DAY OF MARCH 2025

DIRECTOR

SECRETARY

Table of Contents

1.0 Introduction

This policy defines how Information Security will be set up, managed, measured, reported on, and developed within Baobab Microfinance Bank ('Baobab' or 'the Bank').

Baobab has decided to pursue full certification to ISO/IEC 27001 in order that the effective adoption of information security best practices may be validated by an external third party.

1.1 Scope of the ISMS

For the purposes of certification within Baobab, the boundaries of the Information Security Management System are defined as follows:

The scope is defined in terms of the parts of the Bank, products and services, information resources, personnel, and related activities. It covers all critical units within the Bank, namely: Head Office Operations, Admin. & Facility Management, Information Technology, Human Resources, Treasury, Contact Centre, digital channels, Information Security Office, Compliance, Legal Service, Branding, Communications and Marketing, and Internal Audit, Operation and Credit Risk. It also covers the Bank's products and services.

Information Resources include any managed systems, applications, network elements, and any information processed by, or used to provide Information Technology services by the Bank.

The ISMS Scope is limited to the Baobab Nigeria office. The office address in scope is as described below:

Baobab Nigeria
360, Murtala Muhammed Way,
Yaba, Lagos,
Nigeria.

16E Ahmadu Bello Way,
CB Finance House,
Kaduna,
Nigeria.

1.2 The Importance Of Information Resources To Baobab Microfinance Bank

Information resources are vital assets of Baobab Microfinance Bank, as vital as the Bank's other business assets. Information resources are the lifeblood of the Bank and shall therefore be adequately protected against all risks. The protection of Baobab's information resources is critical to Baobab's continuity.

1.3 Why Baobab Microfinance Bank Needs Information Security?

As stated above, Baobab's information resources are critical to its survival. Baobab shall therefore ensure that such information resources are adequately protected when used by all parties authorised to have access to these resources. However, for Baobab to be a competitive player in the market, Baobab shall also share such information resources with other external parties such as customers, vendors, and financial institutions. This reduces the risk that vital Baobab assets will be compromised to the detriment of the organisation.

To protect Baobab's information resources during internal and external use, in addition to conforming to statutory and contractual requirements regarding its information, Information Security is one of Baobab's prime responsibilities in order to protect and secure these vital assets. This responsibility is shared by all employees of Baobab.

1.4 Management's Commitment To Information Security

Information in all its forms, including information about employees, customers and products, is amongst the most valuable assets of the Bank. The security (confidentiality, integrity and availability) of that information is key to Baobab's successful discharge of its responsibilities to customers and stakeholders. Therefore, the security of Baobab's information, the systems and programs that facilitate its use, is a responsibility shared by every employee of the Bank. Every employee of Baobab and extensions of these employees have an obligation to ensure the confidentiality, integrity and availability of Baobab's information resources.

Commitment to information security extends to senior levels of the organisation and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Management is primarily responsible for implementing controls throughout the organisation, in line with corporate governance tenets. Management realises the strategic importance of Information Security within the operations of the Bank. Management hereby gives full support and commitment for the enforcement of all aspects of Information Security on a corporate level as well as that of every individual member's level. This commitment is formulated in terms of the policy statements through the following:

- The Bank shall set up an Information Security Steering Committee, aligning with the CBN cybersecurity framework and guidelines. The Information Security Steering Committee shall be responsible for the governance of the cybersecurity programme, strategy and operations of all Information Security deliverables of Baobab and its subsidiaries.

- Top management will ensure an integration of Baobab's processes with the ISMS requirements and that a systematic review of the performance of the programme is conducted on a regular basis to ensure that quality objectives and the intended outcome of the ISMS are being met, while quality issues are identified through the audit programme and management processes.

- The Bank shall constitute a Change Management/Change Advisory (a management team) that will assess, prioritise and authorise high-risk to minor or low-risk changes to the system & process and schedule changes as part of the change control process.

- Management Review can take several forms, including Senior Management Meetings and other management meetings.

1.4.1 Management Representative

The Information Security Manager/Officer shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

- The identification, documentation, and fulfilment of information security requirements
- Implementation, management, and improvement of risk management processes
- Integration of processes
- Compliance with Information System statutory, regulatory, and contractual requirements
- Reporting to top management on performance and improvement

2.0 Policy statements

Information Security Requirements

2.1 A clear definition of the requirements for information security will be agreed upon and maintained with the business so that all ISMS activity is focused on the fulfilment of those requirements.

2.2 Statutory, regulatory, and contractual requirements will also be documented and input to the planning process.

2.3 Specific requirements regarding the security of new or changed systems or services will be captured as part of the design stage of each project.

2.4 It is a fundamental principle of Baobab's Information Security Management System that the controls implemented are driven by business needs, and this will be regularly communicated to all staff through proper means of communication channels.

Framework for Setting Objectives and Policy

2.5 A 2-year cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle, to ensure adequate funding is obtained for the improvement activities identified.

2.6 Information security objectives will be based upon a clear understanding of the business requirements, informed by the annual management review with stakeholders to ensure that the information security policy and information security objectives are established and compatible with the strategic direction of the organisation.

2.7 ISMS objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on an annual basis to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

2.8 In accordance with ISO/IEC 27001:2013, the control objectives and policy statements detailed in Annexe A of the standard will be adopted, where appropriate, by Baobab.

2.9 These will be reviewed on a regular basis in light of the outcome from risk assessments and in line with the Information Security Risk Treatment Plan. For references to the controls that implement each of the policy statements given, please see the Statement of Applicability.

Business and Information Security Objectives

Business Objectives	ISMS Objectives
Deepen Customer Base in Large, High-Growth & Profitable Market Segments: Baobab will offer unique products with clear value propositions to target distinct market segments, e.g., Product-Based (e.g., ingestibles, body wear, fast-moving electronics) and Service-oriented (e.g., education, entertainment, hospitality, health) entities.	Protection of data of the bank and the customer (Data protection) through Zero tolerance for Cyber breaches.
Reposition the Brand: Baobab will increasingly invest in brand identity and authority.	Consistent and periodic sensitisation on Information Security safety procedures for our customers.
Leverage Tech Platforms & Solutions: Baobab will increasingly localize its digital development and deployment to be more responsive to customer needs and strategically position it as a Neobank.	Deliver our products and services in a secure fashion by performing information security risk assessments and ensuring that 90% of high and critical risks are treated.
Improve on Performance-driven Culture (leveraging KPIS, Competent and Motivated Staff): Baobab will enhance a performance-driven culture through competent, motivated staff focused on managing the key drivers to drive business growth in revenue terms and profitability.	Adequate security awareness at every stage of the employees' journey in the bank, from the onboarding stage onwards. Be a Cyber-aware organisation by ensuring that our workforce attains and maintains a score of 80% in our quarterly information security awareness programs.
Strategic Partnerships and Collaboration: Baobab will embrace partnership opportunities in the market with FinTechs, platform owners, and an open banking model (access to potential customers' data) to increase market share and product development.	Introduce information security from the initial stage to all technology innovations. Ensure that 90% of the exceptions from annual information security audits are implemented within the defined time.

Roles and Responsibilities

2.10 Within the field of information security, there are management roles that correspond to the areas defined within the scope set out above. The full details of the responsibilities associated with each of the roles and how they are allocated within Baobab will be stated in the ISMS Roles, Responsibilities, and Authorities document.

2.11 It is the responsibility of the Information Security Officer to ensure that staff understand the roles they are fulfilling and that they have the appropriate skills and competence to do so.

Continual Improvement

2.12 Baobab's policy with regard to Continual Improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them in line with good practice as defined within ISO/IEC 27001
- Achieve ISO/IEC 27001 certification and maintain it on an ongoing basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) regarding information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them based on collected historical data
- Obtain ideas for improvement via regular meetings with stakeholders and document them in a Continuous Improvement Plan.
- Review the Continual Improvement Plan at regular management meetings in order to prioritise and assess timescales and benefits

2.13 Ideas for improvements may be obtained from any source, including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified, they will be added to the Continual Improvement Plan and evaluated by the staff member responsible for Continual Service Improvement.

2.14 As part of the evaluation of proposed improvements, the following criteria will be used:

- Cost of implementation
- Benefit to the business
- Risk Assessment
- Implementation timescale
- Resource requirement

If accepted, the improvement proposal will be prioritised to allow for more effective planning.

Approach to Managing Risk

2.15 Risk management will take place at several levels within the ISMS, including:

- Management planning – risks to the achievement of objectives

- Information security and IT service continuity risk assessments
- Assessment of the risk of changes via the change management process as part of the design and transition of new or changed services

2.16 High-level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision.

Risk Assessment Process

2.17 A risk assessment process will be used, which is in line with the requirements and recommendations of ISO/IEC 27001, the International Standard for Information Security. This is documented in the Risk Assessment and Treatment Process.

2.18 A risk assessment report will be generated, followed by a risk treatment plan. This will then give rise to the selection of appropriate controls.

Human Resources

2.19 Top management of Baobab is committed to ensuring that all staff involved in information security are competent on the basis of appropriate education, training, skills and experience.

2.20 The skills required will be determined and reviewed on a regular basis, together with an assessment of existing skill levels within Baobab. Training needs will be identified, and a plan will be maintained to ensure that the necessary competencies are in place.

2.21 Training, education, and other relevant records will be kept by the Human Resource Department to document individual skill levels attained. This is to ensure that staff are supported to contribute to the effectiveness of the ISMS.

Auditing and Review

2.22 Once in place, it is vital that regular reviews take place of how well information security processes and procedures are being adhered to. This will happen at three levels:

- Structured regular management review of conformity to policies and procedures
- Internal audit reviews against the ISO/IEC 27001 standard by the Baobab Internal Audit Team
- External audit against the standard in order to gain and maintain certification

2.23 Details of how internal audits will be carried out can be found in the IMS Internal Audit Procedure.

Documentation Structure and Policy

2.24 All information security policies and plans must be documented. This section sets out the main documents that must be maintained in each area.

2.25 Details of documentation conventions and standards are given in the IMS Procedure for the Control of Documented Information.

2.26 Core documents created and maintained as part of the ISMS are to be uniquely numbered, and the current versions will be tracked in the Information Security Management System Documentation Log.

2.27 All information security policies must be communicated within Baobab and be available to interested parties.

Control of Records

2.28 The controls in place to manage records will be defined in the document IMS Procedure for the Control of Records.

3.0 Violation

Any violation of this policy may result in disciplinary action as permitted by the HR Disciplinary Policy. Baobab reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Baobab does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Baobab reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

4.0 References

- General IT Security Policy
- Information Security Policy
- IMS Context, Requirement & Scope

5.0 Revision History

If changes have been made, this table must summarise them for better tracking.

# Change	Pages changed	Description of changes made	Approval date