NCBA GROUP INFORMATION SECURITY AND PRIVACY POLICY STATEMENT

NCBA is a leading corporate group in Africa, with a major presence in Banking, Insurance, Investment, Fintech and Leasing. The Group offers a full range of personal, business and alternate banking channels through its presence in all its markets.

Vision: East Africa's Most Trusted Financial Ally

Senior Management places the highest priority on safeguarding information in every aspect. We recognize that as an organization, we are committed to mitigate information security risks by upholding the confidentiality, integrity, and availability of information. This assurance instils confidence among stakeholders that risks stemming from potential incidents are effectively addressed. Our overarching objective is to consistently enhance the performance of NCBA Information Security and Privacy Information Management System (ISMS & PIMS) throughout the business.

To achieve this, the following information security objectives have been established:

1. Maintain control over user rights and privileges to ensure seamless productivity as NCBA undergoes digitization. Through user education and awareness, we aim to ensure that all stakeholders fully understand and collaboratively manage cyber risks. This strategy also involves cultivating an innovative and expanding cybersecurity team, guided by global best practices.
2. Foster a culture of cyber resilience throughout the organization by integrating secure development practices and robust ICT innovation controls into the ISMS framework. This will ensure the continuous development, implementation, and improvement of secure software and other ICT innovations that are resistant to evolving cyber threats, thereby reinforcing trust and reliability in our products and services.
3. Strengthen defences against all forms of cyber aggression by leveraging modern technology to protect our ICT infrastructure. NCBA will ensure that only authorized individuals and entities have access to our ICT resources.
4. Equip NCBA with the capabilities to effectively respond to evolving cyber threats and incidents, ensuring the protection and resilience of our networks, data, and systems. NCBA will detect, analyse, investigate, and disrupt hostile actions. Additionally, NCBA will empower staff and clients with the knowledge and skills needed to defend themselves.
5. Ensure that all third-party providers with access to the organization's systems, data, or infrastructure are subject to appropriate information security controls. This includes assessing and managing risks related to vendors, partners, and service providers through due diligence, contractual requirements, ongoing monitoring, and compliance with security standards. The objective is to prevent data breaches, service disruptions, and compliance violations originating from third-party relationships.
6. Ensure that all personal data processed by the organization is handled in accordance with applicable data protection laws and regulatory requirements. This includes implementing privacy-by-design principles, conducting Data Protection Impact Assessments (DPIAs), managing data subject rights, and maintaining appropriate technical and organizational controls. The objective is to safeguard individuals' personal information, prevent data breaches, and demonstrate accountability and compliance with standards such as GDPR, local data protection laws, and ISO/IEC 27701.

To achieve these objectives, management shall act to:

1. Make sure information is protected to an appropriate level, based upon its classification and impact of its disclosure, modification or loss.
2. Complying with all relevant information management legislation, regulations and standards.
3. Make 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.
4. Assign the necessary authority for the management, operation, and reporting of ISMS and PIMS performance.
5. Ensure that the resources needed for the ISMS and PIMS are available.
6. Maintaining an ISMS which meets the requirements of ISO 27001:2022.
7. Maintaining PIMS which meets the requirements of ISO 27701:2019.
8. Ensure the continuous improvement of the suitability, adequacy and effectiveness of the information security management and Privacy Information Management systems.

This policy, together with the objectives and targets set, will be reviewed on an annual basis or upon any significant changes to ensure that it remains relevant and suitable for operations of NCBA.

Exceptions to ISMS and PIMS policies will require formal justification and documented risk assessment. The justification must demonstrate a clear business benefit and outline mitigating controls to address any identified security risks.

John Gachora
NCBA Group Managing Director
30th July 2026