SIYANQOBA NGAMANDLA
FINANCIAL SERVICES (PTY) LTD

AML / FICA
COMPLIANCE POLICY

Anti-Money Laundering & Counter-Terrorism Financing

Financial Intelligence Centre Act, 38 of 2001

Company	Siyanqoba Ngamandla Financial Services (Pty) Ltd
Registration No.	2024/830082/07
NCR Registration	NCRCP22239
Compliance Officer	Sphiwe Hlabisa
Version	1.0
Effective Date	1 June 2026
Review Date	June 2027

Document Information

Company	Siyanqoba Ngamandla Financial Services (Pty) Ltd
Registration No.	2024/830082/07
NCR Registration	NCRCP22239
FIC Accountable Institution	Credit Provider — Item 6, Schedule 1, FICA
Compliance Officer	Sphiwe Hlabisa
Document Title	Anti-Money Laundering and Counter-Terrorism Financing Compliance Policy
Governing Legislation	Financial Intelligence Centre Act, 38 of 2001 (as amended)
Version	1.0
Effective Date	1 June 2026
Review Date	June 2027
Physical Address	10 Van Rensburg Ave, Witbank, Emalahleni, 1035, Mpumalanga
Email	admin@siyanqobangamandla.co.za
Telephone	013 590 0421

Purpose of This Document

This policy establishes the framework within which Siyanqoba Ngamandla Financial Services (Pty) Ltd manages its obligations as an Accountable Institution under the Financial Intelligence Centre Act, 38 of 2001 (FICA), as amended by the Financial Intelligence Centre Amendment Act, 1 of 2017, and all applicable regulations and guidance notes issued by the Financial Intelligence Centre (FIC). It sets out the Company's approach to identifying and verifying clients, monitoring transactions, detecting and reporting suspicious activity, and maintaining the records required by law. This policy is read together with the Company's Privacy Policy and PAIA Manual, and is reviewed annually.

1. Introduction and Legal Framework

Siyanqoba Ngamandla Financial Services (Pty) Ltd is a registered credit provider operating under NCR Registration NCRCP22239. As a credit provider extending loans to natural persons, the Company qualifies as an Accountable Institution in terms of item 6 of Schedule 1 to FICA. This classification imposes a comprehensive set of compliance obligations on the Company, including customer due diligence, record-keeping, transaction monitoring, and reporting of suspicious and cash transactions to the Financial Intelligence Centre.

The primary legislation governing this policy is the Financial Intelligence Centre Act, 38 of 2001 as amended. Key supporting instruments include the Money Laundering and Terrorist Financing Control Regulations, the Public Compliance Communications and Guidance Notes issued by the FIC, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004 (POCDATARA), and the relevant provisions of the Prevention of Organised Crime Act, 121 of 1998 (POCA). The Company recognises that non-compliance with FICA carries significant legal, financial, and reputational consequences, and commits to a zero-tolerance approach to money laundering and terrorism financing.

2. Definitions

In this policy, unless the context requires otherwise, the following terms carry the meanings set out below.

"Accountable Institution" means an institution listed in Schedule 1 to FICA, including the Company as a credit provider.

"Beneficial Owner" means the natural person who ultimately owns or controls a client, or on whose behalf a transaction is conducted, as defined in section 21B of FICA.

"Cash Threshold Report (CTR)" means a report submitted to the FIC where a cash transaction equals or exceeds R49 999.99, as prescribed by regulation.

"Client Due Diligence (CDD)" means the process of identifying and verifying the identity of a client and, where applicable, the beneficial owner, and understanding the nature of the business relationship.

"Compliance Officer" means Sphiwe Hlabisa, appointed to ensure compliance with this policy and with FICA.

"Enhanced Due Diligence (EDD)" means additional verification and monitoring measures applied to higher-risk clients, including Politically Exposed Persons.

"FIC" means the Financial Intelligence Centre, established under section 2 of FICA.

"FICA" means the Financial Intelligence Centre Act, 38 of 2001, as amended.

"Money Laundering" means any act or omission that conceals or disguises the proceeds of unlawful activity, as defined in section 4 of POCA.

"Politically Exposed Person (PEP)" means a natural person who holds or has held a prominent public function, and includes their immediate family members and known close associates, as defined in the FIC Act.

"Risk-Based Approach (RBA)" means an approach under which the Company assesses and manages money laundering and terrorism financing risks proportionate to the level of risk identified.

"Suspicious Transaction Report (STR)" means a report submitted to the FIC where there are reasonable grounds to suspect that a transaction involves the proceeds of unlawful activity or is related to terrorism financing.

"Terrorism Financing" means the provision or collection of funds with the intention that they be used to carry out an act of terrorism, as contemplated in POCDATARA.

3. Compliance Officer

The Company has designated Sphiwe Hlabisa as its Compliance Officer for purposes of FICA. The Compliance Officer is accountable to the Information Officer and to the Company's directors for the implementation and ongoing maintenance of this policy. The Compliance Officer is registered with the Financial Intelligence Centre as the responsible person for the Company's FICA obligations.

The responsibilities of the Compliance Officer include overseeing the implementation of and adherence to this policy across all business operations, ensuring that client due diligence procedures are correctly applied, reviewing and approving decisions on high-risk clients and Politically Exposed Persons, receiving and evaluating internal reports of suspicious activity, submitting Suspicious Transaction Reports and Cash Threshold Reports to the FIC as required, maintaining the registers and records prescribed by FICA, ensuring that all relevant staff receive appropriate training, and reporting to the directors on the state of FICA compliance on a quarterly basis.

Compliance Officer	Sphiwe Hlabisa
Appointed by	Director, Siyanqoba Ngamandla Financial Services (Pty) Ltd
Email	sphiwe@siyanqobangamandla.co.za
Telephone	013 590 0421
Address	10 Van Rensburg Ave, Witbank, Emalahleni, 1035, Mpumalanga

4. Risk-Based Approach

The Company adopts a risk-based approach to AML/CFT compliance, as required by the FIC Act Amendment Act of 2017. This means that the Company assesses the money laundering and terrorism financing risks presented by each client relationship and business transaction, and applies controls that are proportionate to the level of risk identified. A higher-risk client or transaction will attract more intensive due diligence, more frequent monitoring, and closer scrutiny, while lower-risk relationships June be managed with standard controls.

The risk assessment takes into account four primary risk dimensions: the nature and purpose of the client relationship; the type of products or services requested; the geographical profile of the client; and the client's background, including whether the client is a Politically Exposed Person or is connected to a high-risk jurisdiction. The overall risk rating assigned to each client — Low, Medium, or High — determines the level of due diligence that must be applied and the frequency of ongoing monitoring.

Risk Category	Typical Profile	Rating
Low Risk	Salaried employee, established employer partner, payroll deduction facility, verifiable income, South African ID	LOW
Medium Risk	Client with limited credit history, income from informal sector, new employer partner not yet verified	MEDIUM
High Risk	Politically Exposed Person, client with previous suspicious activity, foreign national, unusual transaction patterns	HIGH

5. Client Due Diligence

The Company is required by section 21 of FICA to establish and verify the identity of every client before or during the establishment of a business relationship or before concluding a single transaction. No credit facility June be granted and no funds disbursed until the required due diligence has been completed to the Compliance Officer's satisfaction. The Company does not maintain anonymous accounts or accounts in fictitious names under any circumstances.

5.1 Standard Client Due Diligence

For all natural persons applying for credit, the Company must obtain and verify the client's full legal name, identity number from a South African identity document or passport, date of birth, residential address, and contact details. Where a loan is facilitated through an employer partner, the employer's legal name, registration number, and the identity of the person authorising the payroll deduction arrangement must also be verified. All identity documents must be verified against the original or a certified copy, and the Company must cross-reference the identity number against the Department of Home Affairs database or an equivalent verification service.

5.2 Beneficial Ownership

Where a client is a juristic person, including a close corporation, company, or trust, the Company must identify and verify the beneficial owners — that is, the natural persons who ultimately own or control the entity. The Company must obtain information sufficient to understand the ownership and control structure of the entity and must verify the identities of all natural persons holding an ownership interest of 25% or more, or who otherwise exercise effective control.

5.3 Enhanced Due Diligence

Enhanced due diligence must be applied in all cases where a client is identified as a Politically Exposed Person, where the client presents a High risk rating under the Company's risk assessment, or where there are any unusual features in the client's application or transaction history that cannot be readily explained. Enhanced due diligence requires the personal approval of the Compliance Officer before any credit facility is established, the collection of additional information regarding the source of the client's income and wealth, more frequent transaction monitoring throughout the relationship, and senior management sign-off on any decisions to proceed.

5.4 Ongoing Monitoring

Client due diligence is not a once-off exercise. The Company must monitor all client relationships on an ongoing basis to ensure that the information held remains accurate and current, and to detect any transaction patterns that appear inconsistent with the client's stated purpose and financial profile. Client records must be reviewed at least annually for High-risk clients, every two years for Medium-risk clients, and every three years for Low-risk clients. Any significant change in a client's circumstances — including a change of employer, a material change in income, or a change in the nature of transactions — must trigger an immediate review.

6. Identification of Politically Exposed Persons

A Politically Exposed Person (PEP) is a natural person who holds or has held a prominent public function, whether domestically or in a foreign country. This includes heads of state and government, senior government officials, senior judicial or military officials, senior executives of state-owned entities, and senior political party officials. The definition extends to immediate family members of a PEP — including spouses, children, parents, and siblings — and to known close associates who have joint beneficial ownership of a legal entity or close business relations with a PEP.

The Company must screen every new client against publicly available PEP databases and sanctions lists at the point of onboarding and must repeat this screening annually for all existing clients. Where a client is identified as a PEP, the Compliance Officer must be notified immediately, enhanced due diligence must be applied, and the establishment of the credit relationship must be approved in writing by the Compliance Officer. Ongoing monitoring of PEP relationships must be conducted on at least a six-monthly basis. The Company must also screen all clients against the United Nations Security Council consolidated sanctions list and the FIC's targeted financial sanctions lists, and must not proceed with any transaction involving a designated person or entity.

7. Suspicious Transaction Reporting

Section 29 of FICA requires the Company to report to the FIC any transaction where there are reasonable grounds to suspect that the transaction involves the proceeds of unlawful activity or is related to terrorism financing. The obligation to report arises regardless of the amount involved and regardless of whether the transaction was ultimately completed. The obligation to report to the FIC does not replace or suspend the obligation to comply with other applicable laws, including the obligation to report criminal activity to the South African Police Service where appropriate.

7.1 Indicators of Suspicious Activity

In the context of the Company's credit and payroll deduction lending business, the following circumstances June indicate suspicious activity and should prompt internal escalation to the Compliance Officer: a client who is reluctant to provide required identification or who provides inconsistent or implausible information; a client who repays a loan significantly ahead of schedule using a source of funds that cannot be explained; loan applications from multiple individuals sharing the same address, contact details, or bank account; requests for cash disbursements rather than electronic transfers to a verified bank account; any transaction that appears structured to avoid reporting thresholds; and any pattern of transactions that is inconsistent with the client's stated employment status, income, or purpose.

7.2 Internal Reporting Procedure

Any employee of the Company who suspects that a transaction June be suspicious must immediately report this suspicion in writing to the Compliance Officer, providing a full description of the transaction, the grounds for suspicion, and all relevant client information. The Compliance Officer must evaluate the report without delay and, where the grounds for suspicion are substantiated, must submit a Suspicious Transaction Report to the FIC through the goAML reporting platform within the timeframe prescribed by FICA. The Compliance Officer must maintain a register of all internal suspicious activity reports received and all STRs submitted to the FIC.

7.3 Tipping Off Prohibition

Section 32 of FICA strictly prohibits any disclosure to a client or to any other person that a suspicion has been reported or that an investigation is underway. This prohibition, commonly referred to as the tipping-off prohibition, applies to all employees and directors of the Company without exception. Any employee who discloses the existence of a suspicious transaction report, whether intentionally or negligently, commits a criminal offence under FICA. All employees must be made aware of this prohibition as part of their FICA training.

8. Cash Threshold Reporting

Section 28 of FICA requires the Company to report to the FIC any transaction — or a series of related transactions — where the amount in cash equals or exceeds R49 999.99. Given the nature of the Company's business model, which disburses loan funds electronically directly to clients' bank accounts and collects repayments through payroll deductions, the likelihood of cash transactions meeting or exceeding this threshold is low. However, the obligation applies regardless, and any cash transaction of this value must be reported through the goAML platform within three business days of the transaction taking place.

Any employee who receives or disburses cash in connection with the Company's business must immediately notify the Compliance Officer if the amount equals or exceeds R49 999.99, or where a series of related cash transactions collectively reaches this threshold. The Compliance Officer is responsible for submitting the Cash Threshold Report to the FIC and for retaining a copy of the report in the FICA records register.

9. Record-Keeping

Section 22 of FICA requires the Company to retain records of all due diligence information collected, all transactions conducted with or for clients, and all reports submitted to the FIC. These records must be retained for a minimum of five years from the date on which the business relationship ends or the transaction is concluded. Records must be kept in a manner that allows them to be retrieved promptly and provided to the FIC, a supervisory body, or a court upon request.

Record Type	Retention Period	Authority
Client identification and verification documents	5 years from end of relationship	FICA s22
Transaction records (all credit and repayment records)	5 years from transaction date	FICA s22
Suspicious Transaction Reports (copies)	5 years from submission date	FICA s22
Cash Threshold Reports (copies)	5 years from submission date	FICA s22
Internal suspicious activity reports	5 years from date of report	Company Policy
PEP screening records and approvals	5 years from end of relationship	FICA s22
Employee FICA training records	5 years from date of training	Company Policy

Records June be retained in electronic or physical form, provided they are protected against unauthorised access, loss, or destruction. The Compliance Officer is responsible for maintaining an index of all FICA records and for ensuring that they are available for inspection on request.

10. Training and Awareness

Section 43 of FICA requires Accountable Institutions to train their employees to understand the requirements of FICA and to recognise and report suspicious transactions. The Company is committed to ensuring that all relevant employees receive appropriate and regular FICA training, and that training records are maintained for a minimum of five years.

All new employees whose roles involve client interaction, credit assessment, loan disbursement, collections, or financial administration must complete FICA induction training before commencing those duties. Existing employees in these roles must complete refresher training at least annually, or more frequently where the FIC issues material guidance or where legislative changes occur. Training must cover the Company's obligations as an

Accountable Institution, the client due diligence procedures set out in this policy, the identification of suspicious activity indicators, the internal reporting procedure, the tipping-off prohibition, and the personal legal liability that employees June face for non-compliance. The Compliance Officer is responsible for designing, delivering, and recording all FICA training.

11. Non-Compliance and Sanctions

Non-compliance with FICA exposes both the Company and individual employees to serious legal consequences. Under FICA, failure to carry out client due diligence, failure to report suspicious transactions, failure to retain required records, and violation of the tipping-off prohibition are all criminal offences that June attract substantial fines and imprisonment. The FIC also has the power to impose administrative sanctions, including public disclosure of non-compliance, which carries significant reputational risk.

Any employee found to have deliberately circumvented or disregarded the requirements of this policy, or to have facilitated money laundering or terrorism financing, will face immediate disciplinary action, which June include summary dismissal, and June be reported to the South African Police Service and the FIC. The Company will cooperate fully with any investigation by the FIC, the South African Police Service, the Asset Forfeiture Unit, or any other competent authority.

12. Interaction with the Financial Intelligence Centre

The Company's primary channel for interaction with the FIC is the goAML web-based reporting platform, through which all Suspicious Transaction Reports and Cash Threshold Reports are submitted. The Compliance Officer is the registered reporting officer on the goAML platform and is responsible for maintaining the Company's registration details and ensuring that the platform is accessible and operational at all times.

The Company undertakes to cooperate fully and promptly with any request for information, inspection, or audit by the FIC or by any supervisory body acting under the authority of FICA. Where the FIC issues guidance notes, public compliance communications, or directives that are applicable to the Company's business, the Compliance Officer must assess their impact on this policy and on the Company's procedures, and must implement any necessary changes without delay.

13. Policy Review and Updates

This policy is reviewed annually by the Compliance Officer and approved by the directors of the Company. It June also be reviewed at any time in response to changes in applicable legislation, FIC guidance, or the Company's business operations. The current version is distributed to all relevant employees and is retained on the Company's policy register. This version is effective from 1 June 2026 and is due for review in June 2027.

APPROVAL & ADOPTION

This Anti-Money Laundering and FICA Compliance Policy was reviewed, adopted, and approved by the directors of Siyanqoba Ngamandla Financial Services (Pty) Ltd. It will be reviewed annually or upon any material change in legislation or operations.

Document Version	1.0
Effective Date	1 June 2026
Next Review Date	June 2027
Compliance Officer	Sphiwe Hlabisa
NCR Registration	NCRCP22239
FIC Classification	Accountable Institution — Schedule 1, Item 6

Signature: _____ Date: 14/05/2026

Sphiwe Hlabisa

Compliance Officer | Siyanqoba Ngamandla Financial Services (Pty) Ltd

Signature: _____ Date: 13.05.2026

Mkhabela, Nqobile Valentia Veronica

Information Officer | Siyanqoba Ngamandla Financial Services (Pty) Ltd