KYC & AML Policy

Public summary | FIC Act, AML/CFT/CPF and CASP controls

Company	Swoop Financial Solutions (Pty) Ltd
Registration number	2023/883589/07
FSP number	53726
FIC status	Registered Accountable Institution
Website	https://myswoop.co.za
Compliance contact	admin@myswoop.co.za
General email	info@myswoop.co.za
Telephone	+27 72 727 2564
Registered address	17 Lundy Island Avenue, Plettenberg Bay, 6600, South Africa
Effective date	2 June 2026

Version	Owner	Classification	Review
v1.0	Compliance / MLRO function	Public	At least annually or after material regulatory/product change

Contents

1. Purpose and policy statement

This public KYC and AML Policy summarises the anti-money laundering, counter-terrorist financing, counter-proliferation financing and client due diligence controls applied by Swoop. It is intended for clients, prospective clients, service providers, banking partners and other stakeholders who need to understand Swoop's compliance approach.

Swoop is committed to maintaining a risk-based compliance framework, preventing misuse of its services, identifying clients and beneficial owners, screening relevant parties, monitoring client activity, retaining required records and escalating reportable matters to the appropriate responsible persons and authorities.

Public summary

This policy is a public summary of Swoop's control environment. Swoop maintains more detailed internal procedures, including its Risk Management and Compliance Programme, onboarding procedures, monitoring rules, escalation logs and reporting decision records. Those internal procedures are not published because they contain operational and security-sensitive information.

2. Swoop services covered by this policy

This policy applies to Swoop products and workflows that involve client onboarding, crypto asset transactions, fiat settlement, payment facilitation, education/onboarding support, service provider reliance or compliance screening.

Service or workflow	Current control expectation
BTC to ZAR conversion / off-ramp	Client KYC/KYB before use, client screening, wallet/provider information, transaction monitoring, service provider reliance controls and exception escalation.
ZAR to BTC buy flow	Client KYC/KYB before use, bank/payment verification, wallet information, client risk rating, source of funds review and transaction monitoring.
Foreign currency to ZAR using Bitcoin or Lightning as settlement rail	Enhanced product-level compliance review, KYC/KYB, source of funds/source of wealth, sanctions and jurisdiction screening, Travel Rule assessment and SARB/exchange-control confirmation where required.
Bitcoin Under Management education/onboarding	Client onboarding, fit-for-purpose disclosures, risk rating and controls to avoid unauthorised advice or intermediary activity outside Swoop's permissions.
Merchant acceptance, stablecoin or stuck-funds use cases	Not launched unless compliance, legal, service provider, client funds and product approval controls are documented and approved.

3. Regulatory framework

Swoop's KYC and AML framework is designed with reference to South African financial crime and financial sector obligations that apply to its business activities and risk profile.

Area	Swoop control relevance
FIC Act and FIC guidance	Accountable Institution registration, RMCP, customer due diligence, beneficial ownership, ongoing due diligence, recordkeeping, reporting, TFS/sanctions screening and training.
AML/CFT/CPF standards	Risk-based measures to identify, assess, mitigate, monitor and evidence money laundering, terrorist financing and proliferation financing risks.
FAIS / FSCA / CASP obligations	Controls relating to licensed financial services, fit and proper responsibilities, conduct, disclosure, product governance and crypto asset service provider expectations.
Travel Rule	Collection, assessment and transmission or retention of required originator and beneficiary information where a crypto asset transfer falls within Travel Rule requirements.
POPIA and PAIA	Lawful processing, security, retention, data subject rights and access-to-

Area	Swoop control relevance
	information handling for client and compliance records.
SARB and exchange control considerations	Product-level review and external confirmation for cross-border, foreign currency, settlement or exchange-control-sensitive flows.

4. Governance and responsibility

Swoop allocates responsibility for AML/CFT/CPF controls to its management and compliance function. High-risk matters require human review and approval by authorised decision-makers. Automated systems or service provider outputs do not replace accountable human judgement.

Governance area	Control
RMCP	Swoop maintains an internal Risk Management and Compliance Programme that records detailed AML/CFT/CPF procedures, risk assessments and control ownership.
Human approval	High-risk client acceptance, client exits, suspicious/unusual activity decisions, FIC reporting decisions, Travel Rule overrides, client funds issues and product launches require human approval.
Compliance evidence	Swoop maintains registers, client files, screening records, transaction records, decision records, training evidence and service provider oversight evidence.
Review cycle	Controls are reviewed periodically and when Swoop changes products, providers, jurisdictions, client types or regulatory obligations.

5. Risk-based approach

Swoop applies a risk-based approach. This means the level of due diligence, monitoring, approval and evidence required depends on the risks presented by the client, product, geography, transaction pattern, source of funds, source of wealth, wallet type and service provider reliance.

Risk factor	Examples considered
Client risk	Individual, company, merchant, beneficial owner, representative, PEP status, adverse media, sanctions exposure, occupation/business activity and expected activity.
Product risk	BTC-to-ZAR, ZAR-to-BTC, cross-border settlement, Lightning usage, education/onboarding, merchant flows and any new product or material product change.
Geographic risk	Client location, sender/recipient jurisdictions, foreign currency flows, high-risk jurisdictions, sanctions exposure and exchange-control sensitivity.

Risk factor	Examples considered
Transaction risk	Size, frequency, purpose, pattern, funding source, settlement route, counterparties, refunds, reversals, stuck funds and unusual activity.
Wallet and crypto risk	Hosted or self-hosted wallet, wallet provider information, ownership/control evidence, Travel Rule data, blockchain exposure where available and high-risk crypto indicators.
Provider reliance risk	KYC, screening, banking, exchange, liquidity, settlement, wallet, Travel Rule, chain analytics, cloud and support providers.

6. Client onboarding and customer due diligence

Swoop may not provide services until the required onboarding and customer due diligence checks have been completed to Swoop's satisfaction. Swoop may request additional information before, during or after onboarding.

6.1 Individual clients

- identity information and verification evidence;
- contact details and residential address information;
- bank account and payment information where needed for the product;
- wallet address, wallet type and wallet provider information where crypto assets are involved;
- expected activity, transaction purpose, anticipated size/frequency and product use case;
- source of funds and, where required, source of wealth information; and
- screening, risk rating and enhanced due diligence information where applicable.

6.2 Business clients

- company registration, trading, address and tax or regulatory information where applicable;
- director, representative and authorised signatory information;
- beneficial ownership and ownership/control information;
- business activity, customer base, expected transaction activity and product purpose;
- bank account and settlement information;
- wallet, crypto asset and provider information where applicable; and
- source of funds/source of wealth, screening, risk rating and enhanced due diligence information where required.

6.3 Beneficial ownership

For legal persons, trusts, partnerships or similar structures, Swoop takes reasonable steps to identify and verify beneficial owners, controllers and persons acting on behalf of the client. Swoop may refuse or pause onboarding where beneficial ownership, authority or control cannot be adequately established.

7. Screening and enhanced due diligence

Swoop screens clients and relevant connected parties before onboarding and on an ongoing basis. Screening may be conducted directly and through specialist service providers.

Control	How Swoop applies it
Sanctions and TFS screening	Clients and relevant connected persons are screened against sanctions and targeted financial sanctions information. Potential true matches are escalated immediately and may result in transaction blocking, rejection, reporting or exit.

Control	How Swoop applies it
PEP and prominent influential person checks	Domestic PEP, foreign PEP and prominent influential person indicators are considered during risk rating and may trigger enhanced due diligence and management approval.
Adverse media and high-risk indicators	Adverse media, high-risk business activity, high-risk jurisdictions, unexplained transaction activity or inconsistent onboarding information may trigger enhanced review.
Source of funds and source of wealth	Swoop requests and assesses information that explains how the client funds the transaction and, where required, how the client generated overall wealth.
Enhanced due diligence	High-risk clients, unusual product use, unusual transactions, PEP indicators, complex structures or unclear sources of funds may require additional evidence and human approval.
Client rejection or exit	Swoop may reject, suspend, restrict or exit a client relationship where risk cannot be mitigated, information is missing or activity is inconsistent with lawful use of Swoop's services.

8. Transaction monitoring and ongoing due diligence

Swoop monitors client activity to identify transactions or patterns that may be inconsistent with Swoop's knowledge of the client, the client's declared activity, the client's risk profile, or the expected purpose of the product.

Monitoring area	Public control description
Expected activity	Swoop records expected transaction size, frequency and use case during onboarding and uses this to identify activity that may require review.
Manual and system review	Swoop may use manual review, provider alerts, reconciliation checks and other controls to assess transactions and exceptions.
Unusual or suspicious activity	Transactions that appear unusual, complex, inconsistent, unexplained, linked to higher-risk exposure or potentially unlawful are escalated for review.
Ongoing due diligence	Swoop may refresh KYC/KYB, request updated documents, reassess source of funds/source of wealth and update client risk ratings during the relationship.
Operational exceptions	Failed, delayed, reversed, refunded or stuck transactions are reviewed and recorded, especially where client funds or third-party provider reliance is involved.
Confidential controls	Swoop does not publish detailed monitoring rules, thresholds or reporting rationale because doing so could weaken financial crime controls.

9. Crypto asset, wallet and Travel Rule controls

Crypto asset products create specific AML/CFT/CPF risks. Swoop applies wallet, provider, settlement, source-of-funds and Travel Rule controls appropriate to each product and service provider flow.

Area	Swoop control
Wallet information	Swoop may collect wallet addresses, wallet type, wallet provider information and client declarations about ownership or control of wallets.
Self-hosted wallets	Swoop may allow self-hosted wallets, subject to risk assessment, additional information requests, transaction review and escalation where risk indicators are present.
Hosted wallets	Where a client uses a hosted or custodial wallet, Swoop may ask for the wallet or platform provider name and may request further information where required.
Lightning and Bitcoin settlement	Swoop considers the practical data limitations and risks of Bitcoin and Lightning flows and applies compensating controls through onboarding, screening, expected activity, provider reliance and exception review.
Travel Rule	Swoop assesses whether required originator and beneficiary information must be collected, transmitted, retained or reconciled for relevant crypto asset transfers. Missing, conflicting or unverifiable information may result in delay, rejection or escalation.
Provider flow	For certain products Swoop may rely on upstream or downstream service providers for liquidity, exchange, settlement, payment or technical routing. Swoop still maintains its own onboarding, screening, risk assessment and evidence responsibilities.
High-risk crypto exposure	Exposure to fraud, scams, ransomware, sanctioned persons, darknet markets, mixers/tumblers, stolen funds, terrorism financing or other high-risk indicators may result in enhanced review, rejection, blocking, reporting or client exit.

10. Reporting, confidentiality and tipping-off

Swoop maintains internal escalation and reporting procedures for matters that may require reporting to the Financial Intelligence Centre or other competent authorities. Reporting decisions are made by authorised human decision-makers, supported by evidence and internal records.

Reporting area	Public control description
Suspicious or unusual activity	Potentially suspicious or unusual transactions or activity are escalated for review and may be reported where required.
Terrorist property and sanctions	Potential true matches or terrorist property indicators are escalated immediately and handled under applicable reporting and restriction requirements.

Reporting area	Public control description
Cash threshold reporting	Swoop does not operate as a cash business. If cash-related reporting obligations ever become relevant, Swoop will apply the applicable legal requirements.
International and electronic transfers	Cross-border, foreign currency, crypto asset and electronic transfer flows are assessed for applicable reporting, Travel Rule, SARB and partner requirements.
No tipping-off	Swoop personnel and service providers must not unlawfully disclose that a report has been or may be made, or that an investigation is underway.
Regulator cooperation	Swoop cooperates with lawful requests from regulators, law enforcement, banks, auditors and authorised partners, subject to confidentiality, privilege and POPIA controls.

11. Recordkeeping and retention

Swoop retains records needed to evidence compliance, support client services, respond to regulators and maintain an audit trail. Records may be held directly by Swoop or by authorised service providers, provided Swoop can access the records when required.

Record category	Examples
Client due diligence	KYC/KYB records, beneficial ownership, authority evidence, declarations, risk ratings and enhanced due diligence evidence.
Screening and monitoring	Sanctions, TFS, PEP, adverse media, high-risk jurisdiction, alert review and ongoing due diligence records.
Transaction records	Transaction instructions, wallet information, payment records, settlement confirmations, reconciliation records, exceptions and refund records.
Reporting records	Escalation notes, decision records, FIC submission evidence, acknowledgement records, supporting evidence and non-reporting rationale where applicable.
Policy and governance	RMCP, policy approvals, review records, training evidence, internal registers, service provider due diligence and product approval records.

Records are retained for the period required by applicable law and Swoop's retention rules. AML/CFT records are generally retained for at least the statutory period required under the FIC Act after the relevant relationship or transaction, unless a longer period is required for legal, regulatory, audit or dispute reasons.

12. Service provider reliance and oversight

Swoop may use specialist service providers for KYC/KYB, screening, exchange, liquidity, settlement, payment, banking, Travel Rule, wallet, cloud, communication and compliance support. Use of a service provider does not remove Swoop's responsibility to understand and evidence the controls relevant to Swoop's activities.

Provider area	Oversight expectation
KYC/KYB and screening	Provider capability, data quality, screening coverage, audit evidence, POPIA/operator controls and exception handling.
Liquidity, exchange and settlement	Contractual roles, funds flow, crypto asset flow, settlement timing, reconciliation, failed transaction handling and incident escalation.
Payment and banking	Bank account/payment controls, beneficiary/payee controls, reconciliation, refunds, complaints and operational incident handling.
Technology and cloud	Access controls, data security, uptime, backup, incident response, confidentiality and retention controls.
Compliance and legal advisers	Scope of advice, independence, evidence retained, action items and documented management decisions.

13. Client obligations and prohibited activity

Clients must provide accurate, complete and up-to-date information to Swoop. Swoop may delay, suspend, reject or terminate services if information is missing, misleading, unverifiable or inconsistent with Swoop's risk appetite or legal obligations.

13.1 Client obligations

- provide accurate identity, business, beneficial ownership, contact, bank, wallet and transaction information;
- notify Swoop promptly if onboarding information, wallet information, source of funds, expected activity or authorised representatives change;
- provide source of funds, source of wealth, transaction purpose and supporting evidence when requested;
- use Swoop services only for lawful purposes and for the declared purpose;
- cooperate with enhanced due diligence, ongoing due diligence, Travel Rule and provider information requests; and
- not attempt to evade, split, conceal, misrepresent or structure activity to avoid Swoop controls.

13.2 Prohibited or restricted activity

- activity connected to sanctions, terrorist financing, proliferation financing, fraud, scams, ransomware, extortion, theft or proceeds of crime;
- use of false, stolen, nominee, mule or misleading identity, bank, company, wallet or beneficial ownership information;
- transactions involving high-risk exposure that Swoop cannot reasonably mitigate;
- attempts to bypass KYC, screening, monitoring, Travel Rule, source of funds or source of wealth controls;
- activity linked to illegal goods or services, corruption, bribery, tax evasion, market abuse or other unlawful conduct; and
- any activity that Swoop, its providers, banks or regulators identify as outside applicable law, licence conditions, product approval or risk appetite.

14. Training, review and contact

Area	Control
Training	Relevant Swoop personnel receive AML/CFT/CPF, FIC Act, sanctions, suspicious activity, POPIA, Travel Rule and product-specific compliance training appropriate to their roles.

Area	Control
Testing and assurance	Swoop conducts periodic file checks, evidence reviews, provider reviews, monitoring checks and issue remediation where appropriate.
Policy review	This public policy is reviewed at least annually and whenever material regulatory, product, provider or operational changes occur.
Contact	AML/KYC questions may be sent to admin@myswoop.co.za. General enquiries may be sent to info@myswoop.co.za.

This policy should be read with Swoop's Privacy Policy, PAIA Manual, Terms and Conditions and any product-specific disclosures or onboarding requirements.