

# AML Policy

# Contents

- 1. Purpose..... 3
- 2. Scope..... 3
- 3. Definitions..... 3
- 4. Governance & Responsibilities..... 3
- 5. Customer Due Diligence (CDD) ..... 4
- 6. Risk Management..... 4
- 7. Transaction Monitoring & Reporting ..... 4
- 8. Record Keeping..... 4
- 9. Training & Awareness..... 5

## 1. Purpose

The purpose of this AML Policy is to set out the framework by which Swyft Markets complies with the Financial Intelligence Centre Act (FICA), the Prevention of Organised Crime Act (POCA), the Prevention and Combating of Corrupt Activities Act (PRECCA), and international standards as set by the Financial Action Task Force (FATF).

Swyft Markets is committed to preventing its platform from being used for money laundering (ML), terrorist financing (TF), proliferation financing (PF), or any other financial crime.

## 2. Scope

This policy applies to:

- All directors, key individuals, representatives, and employees of Swyft Markets.
- All customers, including natural persons, juristic persons, trusts, and beneficial owners.
- All products and services offered by Swyft Markets (online securities trading).

## 3. Definitions

- Money Laundering (ML): The process of concealing the origins of illicitly obtained funds.
- Terrorist Financing (TF): Providing financial support to terrorism or related activities.
- Politically Exposed Persons (PEPs): Individuals entrusted with prominent public functions, including their immediate family and close associates.
- Beneficial Owner (UBO): A natural person who ultimately owns or controls a client (ownership  $\geq$  5% in line with current FIC guidance).

## 4. Governance & Responsibilities

- Board of Directors: Ultimate responsibility for AML compliance.
- Compliance Officer (MLRO): Responsible for implementing AML controls, reporting suspicious transactions to the FIC, and staff training.
- Employees: Required to comply with all AML procedures, perform due diligence, and escalate suspicions.

## 5. Customer Due Diligence (CDD)

Swyft Markets applies a risk-based approach to CDD.

### 5.1 Identification & Verification

- Collect and verify identification documents (ID, passport, proof of residence, company incorporation docs, beneficial ownership info).
- Electronic verification may be used where available.

### 5.2 Ongoing Monitoring

- Continuous monitoring of client trading activity to detect unusual patterns.
- Review of client risk rating at least annually or upon material changes.

### 5.3 Enhanced Due Diligence (EDD)

EDD will be applied to:

- High-risk clients (PEPs, foreign entities, high-risk countries, crypto-related sources of wealth).
- Clients with complex structures or opaque beneficial ownership.
- Transactions involving large amounts or unusual trading behaviour.

## 6. Risk Management

Swyft Markets maintains a risk-rating framework where clients are risk rated as follows:

- Low Risk
- Medium Risk
- High Risk

## 7. Transaction Monitoring & Reporting

- Automated systems flag unusual trading activity (large volumes, rapid in/out trades, layering activity).
- Suspicious Transaction Reports (STRs) are filed with the FIC as required under FICA.
- Cash Threshold Reports (CTRs) are filed where applicable (cash transactions above R49,999.99).
- Terrorist Property Reports (TPRs) are submitted where required.

## 8. Record Keeping

All CDD records, transaction data, and reporting records are kept for at least 5 years in accordance with FICA.

## 9. Training & Awareness

All staff receive AML training:

- On induction.
- Annually thereafter.
- Ad hoc updates when new regulatory guidance is issued.

## 10. Sanctions & Disciplinary Action

Non-compliance with this policy by employees may result in:

- Disciplinary action, including termination of employment.
- Regulatory sanctions by the FSCA/FIC.
- Criminal prosecution where applicable.

Version 1

<b>Version</b>	V1
<b>Approval date</b>	September 2025
<b>Next Review Date</b>	September 2028
<b>Approved by</b>	Director