# RAA ELITES SACCO SOCIETY LTD.

To promote the economic & social status of our customers in Kenya.

Tel. +254 743 115 040, Email: raaelites@gmail.com

P.O BOX 45 – 60103, RUNYENJES

## ANTI MONEY LAUNDERING POLICY

# Table of Contents

# 1.0 INTRODUCTION

In response to the international community's growing concern with regard to money laundering and the possible financing of terrorism, many countries worldwide have enacted or strengthened their laws and regulations regarding this subject. The Law on preventing the use of the financial system for purposes of laundering money and terrorism financing specifies relevant legal requirements for the financial sector (i.e. credit institutions and a wide range of other financial institutions) to effectively prevent money laundering and the financing of terrorism.

## 1.1 Objectives

The purpose of this policy is to establish the general framework for the fight against money laundering and terrorism financing at RAA ELITES SACCO.
RAA ELITES SACCO is committed to high standards of anti-money laundering/counter-terrorism financing (AML/CTF) compliance and requires management and employees to adhere to these standards in preventing the use of its products and services for money laundering or terrorism financing purposes.

RAA ELITES SACCO AML program shall encompass "Know Your Customer" (KYC) and "Know Your Transactions" (KYT)-rules considered as minimum standards together with procedures transposing these minimum requirements into operational terms and taking into account national regulatory requirements.

## 1.2 Definitions

Money laundering is

i. the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
ii. the concealment or disguise of the true nature, source, location, disposition, movement, or rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity;
iii. the acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
iv. Participation in, association to commit, attempts to commit, and aiding, abetting, facilitating, and counseling the commission of any of the actions mentioned in the foregoing points.

Terrorism financing is the provision or collection of funds and other assets, by any means, directly or indirectly, with a view to, or in the knowledge that those means will be used in full or in part by a terrorist organization or by a terrorist acting alone, even without any connection to a particular act of terrorism.

### 1.3 Governance

The Chief Executive Officer function reports directly to the RAA ELITES SACCO Management Committee which is responsible for SACCO - wide adherence to applicable AML/CFT regulations and obligations.

## 2.0 MINIMUM STANDARDS

Following standards are to be considered as minimum requirements and are elaborated in more detail in other SACCO policy and procedure manuals with respect to “Know Your Customer” and “Know Your Transactions”.

### 2.1 Enterprise-wide Risk Assessment (EWRA)

As part of RAA ELITES SACCO’s risk-based approach, the Society is required to assess on a yearly basis the risks of money laundering and terrorism financing, taking into account risk factors relating to members, geographic areas, products, services, transactions, and delivery channels. These enterprise-wide risk assessments are documented and kept up-to-date.

### 2.2 Know Your Customer (KYC)

***Customer Identification and Verification***

RAA ELITES SACCO has established standards regarding Know-Your-Customer in its membership. These standards require due diligence on each prospective member before entering into a business relationship:

- via identification and verification of his identity and, as the case may be, his representatives and beneficiaries on the basis of documents, data, or information obtained from a reliable and independent source compliant with the anti-money laundering legislation and regulations;
- via obtaining information on the purpose and intended nature of the business relationship

RAA ELITES SACCO does not allow its entities to open anonymous accounts.

***Individual Risk Assessment***

1. The factors taken into account for the individual risk assessment and classification (very high–high-medium-low risk) of our members on a risk-sensitive basis are the ones that are in the scope of the Enterprise-Wide Risk Assessment as mentioned above and relate to the same categories of risk:
    - Delivery channel risk
    - Product, service or transaction risk
    - Customer risk
    - Geographical risk

    Examples of such risk factors that RAA ELITES SACCO is taking into account to assess members as an increased risk of ML/TF and for which enhanced due diligence is applied, are:

    - the home county or county of residence or registration;
    - rank of member
    - the economic activity;
    - the appearance on sanction lists;
    - and beneficiaries;
    - the delivery channel (face-to-face or remotely with or without safeguards);
    - the source of wealth;
    - the type of member;
    - the type and size of payments that could be expected.

2. Customer Acceptance Policy

    RAA ELITES SACCO refuses to establish or maintain a business relationship if the ML/TF risk related to the business relationship appears too high. Therefore, RAA SACCO will not enter into/maintain business relationships if:

    a) It concerns a shell company/bank (entities without any physical presence) or a credit institution or financial institution that allows its accounts to be used by a shell bank.
    b) It concerns cash, cheques, or physical securities without the member being identified face-to-face or identified remotely with safeguards.
    c) It concerns long-term products as long as the member has not been identified, his identity verified and accepted in an appropriate way.
    d) It concerns unlicensed/unregulated platforms.
    e) It concerns arms/munitions dealers.

f) It concerns unlicensed gambling entities.
g) It is not satisfied that the purpose and nature of the business relationship are legitimate.
h) It is not satisfied that the ML/TF risk can be effectively managed, such as no or insufficient identification and verification of the identity of the customer, his representative(s), and/or beneficiaries.
i) The member's source of wealth or source of funds cannot be explained (for example through their occupation, inheritance, or investments).
j) There is no sound economic or lawful rationale for the member requesting the type of financial service sought.
k) The member, his representative is a person or institution appearing on an embargo or terrorist list.
l) The member or anyone associated with them has handled the proceeds of crime.
m) There is in-house negative information about the member's integrity, obtained, for example, in the course of a long-standing business relationship.
n) The member, his representative is a person with whom the RAA ELITES SACCO discontinued the business relationship in the past for AML/TF reasons.

## 2.3 Ongoing Customer Due Diligence

Periodic and risk-based reviews are carried out to ensure that member-related documents, data, or information are kept up-to-date.

## 2.4 Monitoring of Transactions (Know your Transactions (KYT))

The risk management policy and internal control policy should ensure that ongoing transaction monitoring is conducted to detect transactions that are unusual or suspicious compared to the member's risk profile (expected versus real transactional behavior).

This transaction monitoring is conducted on two levels:

a) each business line (first line of control) monitors all customers and their financial behavior and applies enhanced due diligence on those customers who are considered as a higher ML/TF risk;
b) the first line of control is supplemented by a risk-based second line of control, including increased monitoring of transactions of customers regarded as a higher ML/TF risk.

In a number of circumstances described in the KYC rule, measures need to be taken to block the accounts or terminate the business relationship.

### 2.5 Record keeping

Records of personal data obtained for the purposes of the prevention of money laundering and terrorist financing are processed and kept and shall not be further processed in a way that is incompatible with those purposes.

## 3.0 ORGANISATION OF INTERNAL CONTROL

### 3.1 Suspicious Transactions Reporting (STR)

An Internal Auditor is appointed to ensure that unusual transactions that have been detected are reported. The reporting of suspicious transactions must comply with the laws and regulations of the respective local jurisdiction.

### 3.2 Procedures

The Society policies, where applicable must have AML/CTF rules, including minimum KYC standards, into operational procedures taking into account their type of activities, their volume, and their size together with the local legal and regulatory requirements.

### 3.3 Training

The society must put in place a coherent training program, including follow-up training on a regular basis (in-class training, E-learnings, webinars,…), in order to create and maintain a satisfying AML/CTF awareness. The content of this training program has to be worked out in accordance with the kind of business the trainees are working for and the kind of functions they hold.

### 3.4 Compliance Monitoring Program

In order to assure the effectiveness of instructions, procedures, and processes, recurrent quality controls are performed in the AML/CTF domain pursuant to a Compliance Monitoring Program. Reviews and quality controls can be executed by the society at its own initiative.

### 3.5 Reporting

AML/CTF issues and activity reports are submitted on a regular basis to the Supervisory Committee and the BOD. On a yearly basis, the BOD shall assess the quality of coverage of the internal control in this respect.

### 3.6 Internal Audit

Compliance with the policy, the minimum KYC standards, and the procedures that fall within the scope of Internal Audit verify if they are correctly implemented and obeyed.

## 4.0 EXCHANGE OF INFORMATION

The prohibition not to disclose information transmitted to the relevant authorities does not apply

i. between subsidiaries of RAA ELITES SACCO or
ii. towards financial and credit institutions outside RAA ELITES SACCO as long as:
    - cases relate to the same customer and the same transaction.
    - the information exchanged is exclusively used for the purpose of prevention of money laundering or terrorism financing.

The information shared amongst subsidiaries of the Society SACCO is facilitated by the CEO. Adequate safeguards on the confidentiality and the use of information exchanged must be put in place in accordance with the ICT policy.