



AECF ANTI-MONEY LAUNDERING POLICY

Document Review Schedule

Initial Approval

Document Name:	AECF Anti Money Laundering Policy
Document Number:	AECF.2020.06.003
Document Version:	1.0
Document Owner:	Legal
Document Date:	December 2020
Approved By:	AECF Board
Approval Date:	07/12/2020
Effective Date:	07/12/2020

Amendment and Approval

Document Version			
Revision Date:			
Change Description:			
Reason for Change:			
Change Owner:			
Approved By:			
Approval Date:			
Effective Date:			

Amendment Instructions and Version Control

- a) The Initial document is version 1.0
- b) Subsequent amendment / addition of paragraphs will change the second part (0) of the Document Version to 1.1 and increase with subsequent changes in paragraphs
- c) Subsequent amendment / addition of clauses will change the first part (1) of the Document Version to 2.0

Contents

Document Review Schedule	2
Acronyms	4
Definitions	4
1. Purpose	5
2. Scope	5
3. Maintenance & Ownership	5
4. Exceptions to policy	5
5. Policy statement	6
6. References	12

Acronyms

Terms	Description
AML	Anti-Money Laundering
TF	Terrorist Financing
ERM	Enterprise Risk Management
MLRO	Money Laundering Reporting Officer
KYC	Know Your Customer
DD	Due Diligence
MRCC	Management Risk and Compliance Committee
PEP	Politically Exposed Person
BARC	Board Audit and Risk Committee
FRC	Financial Reporting Centre

Definitions

'Money Laundering' Money laundering is the process by which proceeds derived from a criminal activity are disguised in an effort to conceal their illicit origins and to legitimize their future use.

'Terrorist financing' is the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism.

'Politically Exposes Person (PEP)' is defined as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

'Senior political figure' is a senior figure in the executive, legislative, administrative, military or judicial branches of government (elected or non-elected), a senior figure of a major political party, or a senior executive of a government owned corporation. It includes any corporate entity, partnership or trust relationship that has been established by, or for the benefit of, a senior political figure.

'Immediate family' typically includes the person's parents, siblings, spouse, children, in-laws, grandparents, and grandchildren.

'Close associate' typically includes a person who is widely and publicly known to maintain a close relationship with the PEP and includes a person who is in a position to conduct substantial domestic and international financial transactions on the PEP's behalf.

'Shell Company' refers to an institution incorporated in a jurisdiction in which it has no physical presence, and which is unaffiliated with a regulated financial group).

1. Purpose

- 1.1 The objective of this document is to provide guidelines aimed at detecting, identifying and preventing money laundering.
- 1.2 This policy shall also provide guidelines to all staff members on the minimum standards for KYC, Due diligence and transaction monitoring among others.
- 1.3 Laundering is a global problem and organizations in every country are required to strictly comply with money laundering standards. Regulatory Policies across the globe are focused towards strict compliance to AML and KYC Laws/Regulations according to international standards.
- 1.4 The Board of Directors places strong emphasis on having an effective AML Policy and accordingly ensures that AECF has the required tools to achieve this objective. It is the responsibility of all staff to establish additional controls to curb money laundering and strengthen KYC Policies and to protect AECF's reputation by ensuring that its services are not utilized to launder the proceeds of crime.

2. Scope

- 2.1 This Policy shall involve the execution of all procedures and operations that are related to the receipt and transfer of funds by AECF and its employees.
- 2.2 This document is applicable to:
 - 2.2.1 All AECF offices, including the AECF headquarter, branches and desk offices across the Sub Saharan Africa region.
 - 2.2.2 All employees and consultants of AECF, its divisions and subsidiaries.
 - 2.2.3 Funding partners both upstream and downstream.

3. Maintenance & Ownership

- 3.1 The responsibility for the continuous maintenance and ownership of this policy document lies with the Legal Department. This document will be subject to review at least once every 2 years.

4. Exceptions to policy

- 4.1 Policy deviation shall not be acceptable unless a department cannot implement the provisions of a policy as approved by the Board of Directors due to changes in local laws and regulatory environment or where the risk the policy was put in place to manage no longer exists. In such a case, the department should raise an addendum to change the policy.
- 4.2 Exception(s) to this policy must be approved by the Chief Executive Officer or his designate and if of material nature, the Board of Directors must ratify such changes.

5. Policy statement

5.1 Roles and Responsibilities

5.1.1 **The Board Audit & Risk Committee** is the overall body responsible for the monitoring and review of AML Risk Exposures in AECF. This committee is responsible to approving the AML Policy and recommend review where significant changes are required.

5.1.2 **The Management Risk and Compliance Committee (MRCC)** has overall responsibility over continuous monitoring of AML risks in the day to day operations of the organization. The committee shall report all AML incidents to the Executive Committee for further guidance or ratification as may be appropriate.

5.1.3 **Risk Owners (Heads of Departments & the CEO)** are responsible for managing risks in their respective functions. The HODs are required to ensure that AML guidelines are embedded in their policies and incidents of non-compliance are escalated to the MRCC.

5.1.4 **Money Laundering Reporting Officer (MLRO - Head of Legal & Compliance)** shall be responsible for monitoring the implementation and adherence to this Policy. The MLRO is responsible for the general oversight of the operation of this policy, the effectiveness and integrity of suspicious transaction reporting procedures and taking reasonable steps to establish and maintain adequate arrangements for money laundering training.

5.1.5 **All Staff are responsible for**

- obtaining and keep a record of proper and sufficient identification/verification from third parties
- sufficiently ascertain the beneficiaries for all payments made by AECF;
- report suspicious transactions to the MLRO;
- make sure that all applicable laws and regulations are respected.

5.2 Stages of Money Laundering

5.2.1 The first step in laundering process is for the criminals to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity. They can then transfer the proceeds to other accounts, locally and or abroad, or use it to buy goods and services.

5.2.2 It eventually appears to be like any legally earned money and becomes difficult to trace back to its criminal past. The criminals can then invest or spend it or, as often the case, use it to fund more crime.

5.2.3 The laundering process is often described to take place in three stages:

i. Placement – (Injection or Pre-washing)

Placement, being the first stage is the means by which funds from a criminal activity are introduced into the financial system, either directly or through using other retail businesses.

This can be in the form of large sums of cash or a series of smaller sums. Initial proceeds of drug trafficking or street sales of drugs are always in cash.

ii. Layering – (Stacking or Washing)

The aim of the second stage is to disguise the transaction through a succession of complex financial transactions with the purpose of erasing as quickly as possible all links with its unlawful origin. The funds may be converted into shares, bonds or other easily negotiable asset or may be transferred to other accounts in other jurisdictions.

iii. Integration – (Recycling)

Complex integration schemes then place the laundered funds back into the economy through real estate, business assets, securities and equities, in such a way that they re-enter the financial system appearing as normal business funds that have been legitimately earned.

5.3 Prevention of Money Laundering

5.3.1 AECF shall undertake the following in ensuring that ML and TF risks are sufficiently prevented and monitored.

- Establish clear lines of internal accountability, responsibility and reporting.
To this end, AECF shall take primary responsibility for the prevention of money laundering and will ensure that appropriate effective internal controls are in place as well as escalation channels.
- Ensure sufficient KYC documentation is collected from third parties.
AECF shall take all reasonable steps to verify the identity of its donors, investees and contractors. This shall require identification of beneficial owners of all corporate entities (including Trusts), and the principals behind donors or grantees who are acting as agents. AECF will take all reasonable steps to ensure that KYC information about donors and investees collected and kept up-to-date and that identification information is updated when changes occur in the parties involved in a relationship.
- Ensure adequate maintenance and retention of records.
AECF shall establish procedures to retain adequate records of identification for transactions for a minimum of seven years after a relationship has ended. Records relating to training, compliance monitoring and internal and external suspicious transaction reports will also be retained for a minimum of seven years.
- Monitor and report suspicious activities and transactions.
AECF shall make prompt disclosures of suspicious transactions, or proposed transactions, through the appropriate internal channels and, where required to the relevant regulatory authorities. AECF has defined an escalation mechanism in the incident management framework.
- Ensure staff receive adequate training.

AECF shall raise awareness on AML and TF including prevention and train its staff on what money laundering is; the recognition of suspicious transactions; the requirements of regulation and legislation; and the contents of this Policy.

- Co-operate with all lawful government agencies.
AECF shall co-operate with all lawful requests for information made by government agencies during their investigations into money laundering.

5.4 Minimum Document Requirement

5.4.1 AECF shall at minimum collect the outlined documents for KYC purposes.

Information	Documents Acceptable
Identification documents for individuals	Any one of the following in original form or copy certified by a Notary from the county of origin <ul style="list-style-type: none"> - Current Passport or National Identity Card or Driving License or - Army I.D. Card or Alien Certificate and a colored passport size photograph
Identification documents for corporate entities	<ul style="list-style-type: none"> - Certificate of Incorporation - Memorandum and Articles of Association. - Tax compliance Certificate - The full names, date of birth, identity or passport number and address of the natural persons managing, controlling or owning the body corporate or legal entity. - Audited Financial Statements (last full year) at minimum.
Letters of Introduction	<ul style="list-style-type: none"> - In original form, written confirmation from any of the following - - Employer, Leader of registered religious organization, Registered Social Welfare Groups/ Licensed Auditor or a Lawyer - attesting to the - Prospective donor's or grantee's identity - Period they have known the customer (minimum should be 12 months) - Prospective donor's or grantee's physical address
Government Bodies	<ul style="list-style-type: none"> - Signed letter by the CEO/ MD /PS or equivalents detailing the profile of the client and counter signed by the Chairman of the Board

5.5 Classification of AML High Risk parties

5.5.1 Certain characteristics carry much higher money laundering risks as compared with others. Accordingly, the following will be considered high risk;

- Unregulated Charities, NGO and Not for Profit Organizations especially those operating on cross border basis;
- Entities from countries:
 - o subject to sanctions, embargoes or similar measures by the United Nations, the African Union and East African Community;
 - o identified by FATF as not cooperative in the fight against money laundering, or as lacking appropriate money laundering laws and regulations;
 - o identified as providing funding/support for terrorist activities;

- identified as having significant levels of corruption, drug trafficking or other criminal activity.

- Politically Exposed Persons (PEPs)

There is a lot of international attention paid to PEPs, the term given to the risk associated with providing financial and business services to government ministers or officials especially from countries with widely-known problems of bribery, corruption and financial irregularity.

The term 'Politically or publicly exposed persons' will include senior political figures and their immediate family, and close associates.

Examples of PEPs include:

- members of Cabinet;
- senior executives of state-owned corporations;
- important political party officials;
- senior military officials and other members of the disciplined forces;
- members of the Judiciary;
- Senior State Officers; e.g. Cabinet secretaries, House Speakers, Members of the executive,
- Members of public commissions like IEBC, EACC etc.
- Senior Public Officers;
- Senior Official of an International Organization;
- Any immediate family member or close business associate of the above;
- any other category of persons as a country's FRC may determine.

AECF shall conduct a detailed due diligence at the outset of any relationship with a PEP and on an ongoing basis where it is known or suspected that the business relationship is with a 'politically exposed person'. In particular, detailed due diligence for PEP's, should include the following:

- Close scrutiny of any complex structures (for example, involving several companies and/or trusts) so as to establish that there is clear and legitimate reason for using such structures. This is bearing in mind that legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner rather than the reverse.
- Every effort should be made to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship with the Organization.
- Finance – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.
- The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated. A review at senior management level of the decision to commence the business relationship and regular review, on at least an annual basis of the development of the relationship.

- Scrutiny of any unusual features, such as very large transactions in their bank accounts, demands for secrecy, the use of cash or other financial instruments which break an audit trail and regular transactions involving sums just below a typical reporting amount.
- There should be full documentation of the information collected in line with the above.

5.6 Prohibited Customer Types

5.6.1 As a policy, AECF shall not undertake business with:

- Anonymous individuals or institutions
- Individuals or entities subject to UN / OFAC or local country sanctions
- Shell companies
- Companies whose beneficial ownership is not known or not clear
- Unauthorized money changers / prize bond dealers.

5.7 Terrorist Financing

5.7.1 Terrorist financing is the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

5.7.2 Terrorist acts are carried out with the aim of:

- Advancing a political, religious, ethnic, ideological or other cause; or
- Causing fear amongst the members of the public or a section of the public or intimidating or compelling the Government or an international organization to do or refrain from doing an act.

5.7.3 “Terrorist Group” means:

- An entity that has as one of its activities and purposes, the committing of, or the facilitation of the commission of a terrorist act; or
- An entity specified by the government as such.

5.7.4 “Terrorist Property” means:

- Proceeds from the commission of a terrorist act, money or other property which has been, is being or is intended to be used to commit a terrorist act; or
- Money or other property which has been, is being, or is intended to be used by a terrorist group.

5.7.5 The Prevention of Terrorism Act, 2012 provides that a person who knowingly:

- Deals directly or indirectly, in any property that is owned or controlled by or on behalf of a terrorist group;
- Enters into, or facilitates, directly or indirectly any transaction in respect of property referred to at (a) above;

- Provides financial or other services in respect of property referred to in paragraph (a) at the direction of the terrorist group;
- Commits an offence and is liable, on conviction, to imprisonment for a term not exceeding 20 years. All AECF staff must demonstrate that they took all reasonable actions to satisfy themselves that property is not owned or controlled by or on behalf of a terrorist group so as not to be liable in any civil action for any action taken in relation to that property.

5.7.6 AECF shall not engage in business with organizations or countries which are deemed to support terrorist financing.

5.8 Reporting To the MLRO

5.8.1 Where an employee knows or suspects that money laundering&/ terrorist financing activity is taking place or has taken place, the employee must disclose this as soon as is practicable directly to the MLRO. Escalation may also be done through the whistle blower portal on the AECF website or by sending an email to whistleblower@aecfafrica.org.

5.8.2 The disclosure should be within 48 hours of the information coming to the employees' attention.

5.8.3 Failure to do so may amount to a criminal offence in certain jurisdictions. In any event, any employee who fails or neglects to report suspected money laundering activities shall be subject to disciplinary action in line with AECF's Human Resources policies.

5.9 Review of Disclosure Reports by MLRO

5.9.1 Upon receipt of a report, the MLRO must note the date thereon and acknowledge receipt of the report. The MLRO will consider the report and any other available internal information and undertake reasonable inquiries into the issue and report to the MRCC not later than 3 business days (Where MRCC is not scheduled to sit within the 3 days, escalation must be done by e-mail). Escalation must also be done to the chairman of the BARC by MLRO.

5.9.2 Where an investigation is deemed necessary, the Head of Internal Audit shall be the lead and together with the Head of Legal, shall liaise with any investigative bodies as necessary. A detailed investigations guideline has been embedded in the Internal Audit Manual.

5.9.3 If the MLRO knows, suspects or has reasonable grounds to suspect that money laundering activity is taking place, through a disclosure made to them, and does not disclose this as soon as is practicable to the country's Financial Reporting Centre, then he may be liable to an inquiry and disciplinary action.

5.10 Regulatory Reporting

5.10.1 Where the MRCC concludes that the matter is to be forwarded to a regulatory reporting or investigative agency, it must be done within 7 days in the manner prescribed by the laws of the relevant country. Where MRCC concludes that there are no reasonable grounds to suspect money laundering, it shall mark the report accordingly. All disclosure reports referred to the MLRO and those made by him to the Reporting Agency must be retained by the MLRO in a confidential file for that purpose for a minimum of 7 years.

5.11 **Tipping Off**

- 5.11.1 During an ongoing investigation, employees should not tip off any part under investigation. Tipping-off is considered a Money Laundering - related offense under the Proceeds of Crime and Money Laundering Law of Kenya, and other related international guidelines.

5.12 **Exiting a Relationship**

- 5.12.1 AECF shall not enter into or maintain relationships that it believes may be used or are being used for money laundering purposes. Where suspicion of money laundering is established and on the advice of the MLRO, Management shall take immediate steps to terminate AECF's relationship with the counterparty. Where an external disclosure has been, or is being made, care should be taken in exercising the option to terminate; as such an action may alert the donor or grantee and prejudice official investigations.

6. References

- 6.1 The AML Policy should be read in conjunction with:
 - 6.1.1 The Code of Business Conduct and Ethics
 - 6.1.2 Internal Audit Manual
 - 6.1.3 Human Resource Policy
 - 6.1.4 Enterprise Risk Manual