PLATCORP HOLDINGS LIMITED

Anti-Money Laundering (AML), Know Your Customer (KYC) and Combating the Financing of Terrorism (CFT) Policy

Document History

Version	Year	Description	Approval Date
1.0	2018	AML, KYC and CFT Policy	5th March 2018
2.0	2021	AML, KYC and CFT Policy	27th October 2021
3.0	2023	AML, KYC and CFT Policy	17th May 2023

1. INTRODUCTION

1.1 Platcorp Holdings Limited and its subsidiaries, (hereinafter 'the Company') is committed to the compliance of recognized global standards on combating money laundering and terrorism financing.

1.2 Internationally, initiatives to prevent the misuse of financial systems by persons laundering money and financing terrorism led to the formation of the Financial Action Task Force (FATF). FATF is an intergovernmental policy making body which sets standards, develops and promotes policies to combat money laundering and terrorism financing. In 2012, FATF revised and issued 40 recommendations on combating money laundering and terrorism financing. These are recognized as the global standards on combating money laundering and terrorism financing and it has become basis for framing Anti Money Laundering and combating financing of terrorism policies, procedures and controls by the various governments both locally and regionally.

1.3 In addition to this, reference is also made to recommendations of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).

1.4 Compliance with these standards by the Company has become necessary for both local and regional financial relationships.

1.5 The guidelines also incorporate aspects covered in the Basel Committee document on customer due diligence which is a reflection of the International Financial Community's resolve to assist law enforcement authorities in combating financial crimes.

1.6 This policy document is therefore prepared in cognizance of the anti-money laundering and combating of terrorism laws and regulations across all jurisdictions that the company operates.

2. OBJECTIVES

2.1 To lay down policy framework for abiding by Anti Money Laundering Measures, Know Your Customer norms and Counter Financing of Terrorism as set out in the act.

2.2 To comply with applicable anti-money laundering and combating financing of terrorism laws and regulations across all the jurisdictions that the company operates.

2.3 To set out procedures that prevent the Company from being used intentionally or unintentionally as a conduit by criminal elements for money laundering, terrorism financing activities.

2.4 Enabling the Company to know / understand its customers and their financial dealings better, which in turn would help it to manage its risks prudently.

2.5 Conducting due diligence in respect of customers and reporting of any suspicious transactions.

2.6 To ensure that all employees are aware of the existing legislations on AML/ CFT and any changes that have been made, their responsibilities regarding these changes and the consequences of non-compliance.

3. SCOPE OF THE POLICY

3.1 This policy is applicable across all subsidiaries / business segments of the Company and is to be read in conjunction with related operational guidelines issued from time to time.

3.2 The contents of the policy shall always be read in tandem/auto-corrected with the changes / modifications which may be advised by the governments of jurisdictions where the Company operates from time to time.

4. DEFINITIONS

4.1 Customers

For the purpose of this policy, a customer is defined as:

a) A person or entity that maintains and/or has a business relationship with the Company

b) Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company

4.2 Money Laundering

Money Laundering means the act of a person who:

a) Engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity
b) Acquires, receives, posses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Kenya proceeds of any unlawful activity or;
c) Conceals, disguises or impedes the establishment of the true nature, origin, location, movement, deposition, title of rights with respect to, or ownership of proceeds of any unlawful activity where

i. As may be inferred from objective factual circumstances, the person knows or has reason to believe, that the property is proceeds from any unlawful activity or
ii. In respect of the conduct of a natural person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property is proceeds from any unlawful activity. (Persons means any natural or legal entity)

4.3 Beneficial Owner (BO)

The term beneficial owner has been defined as the natural person who ultimately owns or effectively controls a customer and /or the natural person on whose behalf a transaction is conducted.

4.4 Terrorism Financing

Relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism.

4.5 Suspicious Transaction

Suspicious transaction means a transaction which includes exchange or transfer of funds in whatever currency, whether in cash or by cheque or other instruments or other non-physical means including an attempted transaction, whether or not made in cash, which to a person acting in good faith:

a) Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the schedule of AML Act regardless of value involved.
b) Appears to be made in circumstances of unusual or unjustified complexity.
c) Appears to have no economic rationale or bonafide purpose.
d) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism:

5. ROLES AND RESPONSIBILITIES

Employees and other internal stakeholders have a responsibility to ensure that the KYC, AML & CFT compliance program runs smoothly.

5.1 Board of Directors

a) Ensure that the company has in place an AML/ KYC & CFT policy which is consistent with the law and approve all other relevant policies and procedures that address money laundering and terrorist financing risks.
b) Overseeing the KYC, AML and CFT Program on at the highest level.

c) Set the risk appetite for KYC, AML & CFT related risks.
d) Receiving regular status reports on the KYC, AML and CFT Program.
e) Empowerment of the duly appointed Money Laundering Reporting Officer (MLRO) Officer with the necessary authority and resources to carry out the function.

5.2 Senior Management

a. Ensure that an effective AML Program that addresses money laundering and terrorism financing risks is in place; and ensure it enhances the ability of the company to identify, monitor, and deter persons from attempting to gain access to, or make use of the financial system;
b. Provide for and document procedures to perform checks to measure compliance with the relevant AML laws and regulations;
c. Approve the establishment or continuation of a business relationship with a customer that is profiled as high risk; including approving termination of
d. relationships with existing customers that have been subjected to sanctions;
e. Provide for and document AML training for all staff;
f. Provide for adequate screening procedures to ensure high ethical and professional standards when hiring staff;
g. To appoint an MLRO who shall be of management level and shall have relevant and necessary competence, authority and independence.
h. To report to the relevant regulatory bodies in the jurisdiction in which the company operates, within fourteen days of the appointment or removal of the MLRO.
i. Ensuring that MLRO is promptly advised where there are reasonable grounds to know or suspect that transactions or instructions are linked to criminal conduct, money laundering or terrorist financing.

5.3 Role of Anti-Money Laundering Reporting Officer (MLRO)

a) Developing and maintaining the AML and CFT Compliance Program, which includes regularly reviewing and maintaining a record of all relevant updates and documentation;

b) Ensuring that all employees and other relevant parties receive appropriate AML and CFT training at least annually;

c) Reporting to the Board and Senior Management on the status of the AML Program, including any AML Compliance Effectiveness;

d) Corresponding with the relevant regulatory bodies[1] on matters relating to AML and CFT; and file and maintain the relevant compliance reports with the regulatory bodies.

e) Maintaining up to date knowledge of relevant AML and CFT requirements as they apply to the company's business; and

f) Receive and review reports on suspicious activities and file reports on disclosures deemed suspicious to the relevant regulatory bodies in the manner provided for by the regulations.

6. KNOW YOUR CUSTOMER STANDARDS

6.1 Each Company shall document KYC procedures that will ensure that the Company know/understand customers and their financial dealings better

6.2 The procedures shall be based on the following eight pillars:

a) Customer Acceptance Policy (CAP)
b) Customer Identification Procedures (CIP)
c) Customer Due Diligence;
d) Ongoing Due Diligence
e) Enhanced Due Diligence
f) Risk Management
g) Staff Training
h) Responsibilities, Accountability and Reporting
i) Records Retention
j) Suspicious Transaction Reporting

7. PILLARS OF AML / CFT POLICY

7.1 Customer Acceptance Policy (CAP)

~~a)~~ The Company shall accept customers strictly in accordance with this policy.

b) Sanctions; The company shall apply necessary checks to ensure that the identity of the customers or entities does not match with any person with known criminal backgrounds or with banned entities in accordance with UN Sanction (1267) List, Office of Foreign Assets

[1] Relevant Regulatory Bodies include: Kenya- Financial Reporting Centre (FRC); Uganda- Financial Intelligence Authority (FIA); Tanzania- Financial Intelligence Unit (FIU); South Africa- Financial Intelligence Centre (FIC); Zambia- Financial Intelligence Centre (FIC); and Lesotho- Financial Intelligence Unit (FIU): Mauritius- Financial Intelligence Unit (FIU); Democratic Republic of Congo- Financial Intelligence Unit (FIU)

Control Sanction (OFAC) List, European Union (EU) Sanction List, and other relevant Sanction Lists.

c) Politically Exposed Persons- A politically exposed person(PEP) means a person who has been entrusted with a prominent public function in a country. This includes but is not limited to the following:

i. Members of the Executive (President, Deputy President) of the country.
ii. Senior members of the Cabinet including Cabinet Secretaries, Principal Secretaries and Chief Administrative Secretaries;
iii. Senior executives of state-owned corporations;
iv. Senior Executives at the County Government
v. Important political party officials;
vi. Senior military officials and other members of the disciplined forces;
vii. Senior members of the Judiciary;
viii. Senior State Officers and Senior Public Officers i.e of an International organization such as UN, WHO, World Bank, IMF etc.;
ix. Any immediate family member or close business associate of a person referred to above; and
x. Any other category of persons as may be determined by the regulators.

d) PEPs are deemed to present high risk and the company shall apply enhanced due diligence when dealing with PEP and ongoing monitoring of business relationship.

7.2 Customer Identification Procedure (CIP)

Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, *to their satisfaction*, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship.

The customer's identification documents such as a national ID, shall be verified via government databases such as the Integrated Population Registration System (IPRS) database in Kenya.

Being satisfied means that the organization is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the respective laws and regulations.

Besides risk perception, the nature of information/documents required would also depend on the type of the customer.

7.3 Customer Due Diligence

With a view to have a thorough understanding about the customers and the nature of their activities, the company shall obtain relevant information on sources of funds at the time of establishing initial business relationship to understand their normal and expected activity.

Based on due diligence conducted, the company shall maintain risk profiles of all its customers and keep them up-dated. The risk profile of all prospective customers shall be assessed as part of AML/ TF risk assessment and the ongoing KYC and monitoring procedures will be set according to that risk.

7.3.1. Guiding Principles for the Company;

a) Do business with customers whose status and identity is fully known as well as source of funds
b) Determine identity and maintain risk profile, background and business records of all customers.
c) Regularly monitor business relationships and keep customer risk profiles and records updated.

7.3.2. The Company policy is to identify customers:

a) When establishing initial business relations.

b) When undertaking occasional or one-off transactions.

c) When there is cause to be suspicious.

d) When there is doubt about veracity or adequacy of previously obtained identification information.

7.4 Due Diligence on Individual Customers

In conducting due diligence for individual persons, the company shall obtain the following;

a) Valid identification documents
b) Additional measures that may be used to identify and verify the identity of the customer include postal address, current physical or residential address; source of income; Bank statements, Pay

slips, nature and location of business activity, income tax personal identification number (PIN)

The company shall ensure that due diligence conducted at onboarding is line with the risk profile of the customer.

7.5 Due Diligence on legal Persons

The company shall obtain the following in seeking to establish the identity of a legal person or other body corporate

a) its registered name;

b) evidence of registration or incorporation such as a certified copy of Certificate of Registration or Certificate of Incorporation, or Memorandum and Articles of Association or other similar documentation evidencing the legal status of the legal person or body corporate;

c) certified copy of board resolution stating authority to open an account or transact business with the reporting institution, and designating persons having signatory authority thereof;

d) 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

e) Company's personal identification number (PIN)

7.6 Due Diligence on Trusts

The company shall obtain the following particulars in seeking to establish the identity of trust;

a) its registered name, if any;

b) its registration number, if any;

c) evidence of registration or incorporation such as a Certificate of Incorporation or registration;

d) trust deed;

e) formative document such as partnership agreement, memorandum and articles of association;

f) official returns showing registered office and if different the principal place of business;

g) full names and details of the management company of the trust or legal arrangement, if any;

h) names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement;

i) full names of trustees, beneficiaries or any other natural person exercising ultimate effective control over the trust;

j) full names of the founder of the trust and KYC documents

k) any other documentation from a reliable independent source proving the name, form and current existence of the customer;

7.7 Prohibited Customer Types

As a policy, the company does not undertake business with:

a) Anonymous customers

b) Individual or entities subject to International or local country sanctions

c) Shell corporations

d) Customers hiding beneficial ownership of the account or transaction

7.8 Declining Customers

Where the company is unable to fully comply with the customer due diligence requirements, it:

a) Shall not commence the business relationship or perform or undertake the transaction; or

b) In the event the company has already commenced the business relationship, terminate the business relationship; and

c) File a suspicious transaction report in accordance with the regulations.

7.9 Beneficial Ownership

a) The company shall ensure that it is able to identify and verify the natural persons behind legal persons and arrangements.

b) In addition, the company is required to understand the nature of business, ownership and control structure when performing Customer due diligence (CDD) measures in relation to customers that are legal persons or legal arrangements.

c) The objective of undertaking this function would be to identify the natural persons exercising control and ownership in the legal person or arrangement. Information that may be obtained from customers to assist the company in this function includes the following:

i. Certificate of incorporation
ii. Partnership agreement
iii. Deed of Trust
iv. Memorandum and Articles of Association
v. Official returns showing registered office and if different the principal place of business
vi. Names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement
vii. Names of the trustee, beneficiaries or any other natural person exercising ultimate effective control over the trust.
viii. Any other documentation from a reliable independent source proving the name, form and current existence of the customer.

d) The relevant identification data may be obtained from a public register, from the customer or other reliable sources.

7.10 Ongoing Customer Due Diligence

The company shall ensure that its ongoing customer due diligence processes helps to identify, mitigate and manage ML/ TF risks. Transaction monitoring program shall be commensurate with the risk profile of the customer. Additional customer information and beneficial owner information shall be collected and verified on an ongoing basis.

7.11 Enhanced Due Diligence

Enhanced due diligence measures shall be applied to persons and entities that are perceived to present a higher ML/TF risk to the company

This can broadly be addressed with the following measures:

a) Obtain further information to establish the customer's identity.

b) Apply extra measures to check documents supplied by the customer

c) Obtain senior management approval for the new business relationship or transaction.

d) Establish the person’s/entity’s source of funds.

e) Carry out ongoing monitoring of the business relationship

7.12 Risk Management

a) This AML & CFT policy and related procedures cover management oversight, systems and controls, segregation of duties, training and other related matters which ensure effective AML & CFT risk management and implementation of the Company's AML & CFT policy.

b) AML and CFT risk assessments shall be conducted for all new products, services and matters raised in the assessment shall be satisfactorily addressed prior to launch of the product/service.

c) The company shall employ a risk based approach to assess the perceived risk that is likely to be posed by potential customers i.e., new and existing customers, which takes into account the type of products; nature of the customer's business; geographical location of the customer, their business or bank accounts; preferred mode of payments/ delivery channels; volume of transactions; sources of funds; and type of customer e.g., high net worth customers or peps etc.

7.13 Staff Training

a) Risk & Compliance department shall ensure that all staff members are provided with relevant training periodically in phases on applicable Anti Money Laundering Laws and recent trends in money laundering activity as well as the company's policies and procedures to combat money laundering
b) Training shall be tailor-made depending on the job role.
c) Staff Training Records will be maintained in form of a register and shall as at a minimum contain the following information:
    - Duration of training
    - Subject areas covered
    - Highlights of key topics covered
    - Mode of delivery i.e. physical or virtual
    - List of participants and signed off by them.

7.14 Responsibilities, Accountability and Reporting

a) The Company shall ensure adherence to the KYC, AML & CFT policies and procedures.
b) Internal Audit function shall specifically review the application of KYC, AML and CFT Policy and Procedures and comment on the lapses if any observed in this regard.

7.15 Records Retention

The Company shall at all times ensure that it maintains and keeps records of all transactions for a minimum period of ten years from the date the relevant business or transaction was completed or following the termination of an account or business relationship.

These shall include records obtained through customer due diligence measures such as copies or records of official documents like passports, identification cards or similar documents, account files and business correspondence including the results of any analysis undertaken such as inquiries to establish the background and purpose of complex, unusual, large transactions.

In the event where customer accounts are involved in litigation, the company will retain these documents either for as long as is required by courts of law or up to conclusion of matters.

7.16 Suspicious Transaction Reporting

a) Where the company becomes aware of suspicious activities or transactions which indicate possible money laundering or terrorism financing, the company shall ensure that it is reported to the relevant regulatory bodies immediately or within seven days of the date of the transaction or occurrence of the activity that is considered suspicious.

b) It is the duty of every member of staff to report to MLRO any suspicious transactions or activity including where there are reasonable grounds to know or suspect. A guide to what could be construed as a Suspicious Transaction shall be provided to all staff

c) A review shall be undertaken by the MLRO to establish whether there is need for further investigation, or whether there is additional information that removes the suspicion

d) IF the transaction Is deemed to be suspicious, the MLRO shall report the same to the relevant regulatory bodies in the manner prescribed by the regulations

e) The Suspicious Transaction Report shall provide sufficient details, regarding the activities or transactions so that authorities can properly investigate and, if warranted, take appropriate action.

7.17 Tipping Off

Where the company obtains or becomes aware of information which is suspicious or indicates possible money laundering activities, it shall not disclose such information to the customer but shall, report it to the relevant regulatory bodies as required by the guidelines

8. POLICY UPDATE AND REVIEW

This policy will be reviewed every two years and any revised version shall be submitted to the Board for approval.

9. BOARD APPROVAL

This policy is approved by the Company's Board of Directors on 17/05/2023

Signed by:

Chairman: _____ **Date: 17/05/2023**

REFERENCE LEGISLATIONS, REGULATIONS & GUIDELINES:

KENYA:
Proceeds of Crime & Anti-money Laundering Act, (No. 9 of 2009) (Revised 2022)
Proceeds of Crime & Anti-money Laundering Regulations, 2013
Prevention of Terrorism Act (2012)
Prevention of Terrorism Regulations (2013)

UGANDA:
Anti-Money Laundering Act, 2013
Anti-Money Laundering (Amendment) Regulations, 2022
The Anti-Money Laundering (Exchange of Information) Regulations, 2018
Anti-Terrorism (Amendment) Act (2015)
Anti-Terrorism Regulations (2016)
Penal Code Act
The Anti-Corruption Act, 2009
The Narcotic Drugs and Psychotropic substances (Control) Act 2016
Financial Institutions Amendment Act, 2016
Data Protection and Privacy Act 2019

TANZANIA:
Anti-Money Laundering Act, Cap. 423 of 2006 - for Tanzania Mainland (AMLA)
Anti-Money Laundering and Proceeds of Crime Act, No. 10 of 2009 - for Tanzania Zanzibar (AMLPOCA)
AMLA Regulations, June 2022
The Anti-Money Laundering (Electronic Funds Transfer and Cash Transactions Reporting) Regulations, 2019.
The Anti-Money Laundering (Cross-Border Declaration of Currency and Bearer Negotiable Instruments) Regulations, 2016.
Anti-Money Laundering and Proceeds of Crime (AMLPOCA) Regulations 2015
Prevention of Terrorism (General) Regulations, 2014

SOUTH AFRICA
Financial Intelligence Centre Act
Prevention of Organised Crime Act, (POCA),
The Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA Act),
The South African Police Service Act, (SAPS Act)
National Strategic Intelligence Act.
Money Laundering and Terrorist Financing Control Regulations, 2002,

ZAMBIA
Anti_Corruption_Act_2010
Anti_Terrorism_Act_2007
FIC_Amendment_Act_4_of_2016

Financial Intelligence Centre Amendment Act No. 16 of 2020
Financial_Intelligence_Centre_Act_2010
Forfeiture_of_Proceeds_of_Crime_Act
General Regulations S.I. No. 9 of 2016 National_Payment_Systems_ACT_No_1_2007
Prohibition and Prevention of Money Laundering Act_2001
Public_Interest_Disclosure_Protection_of_Whistleblowers_Act_2010
SI No52 Prescribed Thresholds
SI No53 Prescribed Threshold Regulations 2022
SI No53 Prescribed Threshold Regulations 202
SI No54 General Regulations 2022.PDF)

LESOTHO

Money Laundering and Proceeds of Crime (Amendment) Act No. 7 of 2016
ML Regulations No. 29 of 2019
Money Laundering (Amendment) Regulations No. 38 of 2019
Money Laundering (Politically Exposed Persons) Guidelines 152 of 2015
Money Laundering (Financial Sanction Relate Terrorist of Proliferation) Guidelines No 6 of 2022
Money Laundering (Accountable Institutions) (Amendment) Guidelines 2014