COINPLUG KYC/AML/CFT POLICY

TABLE OF CONTENTS

GLOSSARY OF TERMS

1. **AI:** Artificial Intelligence
2. **ML:** Money Laundering
3. **NFIU:** Nigeria Financial Intelligence Unit
4. **AML:** Anti-Money Laundering
5. **SMB:** Small and Medium-Sized Businesses
6. **API:** Application Programming Interface
7. **KYC:** Know Your Customer
8. **CBN:** Central Bank of Nigeria
9. **CTF:** Combating Terrorist Financing
10. **MLR:** Money laundering Report
11. **MLCO:** Money Laundering Compliance Report
12. **Key Personnel:** Refers to any employee of the Company in a position that involves contact with Customers or reviews the Transactions.
13. **LOB:** Line of Businesses
14. **UBO:** Refers to the Ultimate beneficial owner, i.e. the natural person on whose behalf the transaction is executed by a Customer
15. **PEPs:** Politically Exposed Persons
16. **CUSTOMER:** Vendors, beneficiaries.
17. **COMPANY/COINPLUG:** COINPLUG DIGITALS LTD.

INTRODUCTION

Coinplug is dedicated to establishing and upholding effective internal controls to halt money laundering and terrorist funding schemes. The company has a zero-tolerance policy for these behaviors and is required to abide by the pertinent regulations aimed to prevent anti-money laundering and countering terrorism financing (commonly known as "AML/CTF"). These regulations include the Money Laundering (Prevention and Prohibition) Act of 2022 and AML/CFT guidelines.

This policy outlines Coin plug obligations regarding adhering to, complying with, and upholding anti-money laundering ("AML") and counter-terrorist financing ("CFT") laws. It also provides information and guidance to all coinplug employees, including contractors, vendors, donors, users, beneficiaries, and business partners, on how to identify and address any potential money laundering/terrorist financing issues if they arise.

This Policy might be modified occasionally to reflect changes to the laws and rules it is based on.

OBJECTIVES

The Money Laundering (Prevention and Prohibition) Act of 2022, the Cybercrimes (Prohibition, Prevention, ETC) Act of 2015, the Advance Fee Fraud Act, and the Terrorism (Prevention and Prohibition) Act of 2022 with the key stakeholders, geared to ensure that Land TF are combated, has put the essential systems and procedures in place.

The following are the primary aims of this Policy:

i. To guarantee that every precaution is taken top recent ML and FT activities.

ii. To ensure that know Your Customer (KYC) data is gathered and regularly updated.

iii. To make sure guide lines set out by the Nigeria Financial Intelligence Unit (NFIU) and the Central Bank of Nigeria (CBN) are strictly adhered to.

iv. Ensure that all monies (crypto currency) are used for the sole purpose which it was released for.

v. To ensure that vendors and donors don’t use the platform to launder money or fund terrorism.

Account holders, Users, Vendors, Donors, Businesses, Beneficiaries, Partners, third parties, and anybody working with Coinplug on a paid or unpaid basis are

all considered Customers of coinplug and are subject to the terms of this Policy. Customer or any other relationships whatsoever with Coinplug ,will be terminated for any violation of this Policy.

SCOPE

Money laundering is the process of converting money or other assets (criminal property) obtained through criminal activity into "clean" money or other assets with no overt sign of their illicit origins. Any type of asset can be considered criminal property, including cash or its equivalents, securities, physical products, and intangible assets.

Terrorism financing is providing, depositing, distributing, or collecting money directly or indirectly with the knowledge that it would be used entirely or in part to finance terrorism.

The AML/CFT Policy of the Company is targeted at preventing and detecting money laundering and the financing of terrorism, as well as any activity that facilitates them, in accordance with all applicable legal and regulatory requirements. This general policy document applies to all services provided by the Company and to all Customers of these service

The AML/CFT Policy defines the Company's identification and surveillance procedures, the procedures for integrating new Customers and monitoring existing Customers, the CDD tools, the methods for assessing risks, monitoring transactions, and reporting unusual or suspicious activities, the asset freezing system, the procedures set out for the Documents archiving, the means of ensuring ongoing training of the key personnel and the internal control system.

In addition to this internal policy, the AML/CFT system of the Company includes Risk Assessment.

All those who fit into the following groups are seen to be particularly vulnerable to engaging in money laundering and/or financing terrorism:

a. Politically Exposed Persons (PEPs);

b. Participation in an organized criminal group and racketeering;

c. Terrorism, including terrorist financing;

d. Tracking human beings and migrant smuggling;

e. Sexual exploitation, including sexual exploitation of children;

f. Illicit tracking in narcotic drugs and psychotropic substances;

g. Illicit arms tracing;

h. Illicit tracking in stolen and other goods;

i. Corruption and bribery;

j. Fraud;

l. Counterfeiting currency;

m. Counterfeiting and piracy of products;

n. Environmental crime;

o. Murder, grievous bodily injury;

p. Kidnapping, illegal restraint, and hostage-taking;

q. Robbery or theft;

r. Smuggling;

s. Extortion;

t. Forgery;

u. Piracy, Insider trading, and market manipulation.

Our Policy

ML-TF Mitigating Measures

The characteristics of the Services limit their exposure to ML/FT risks:

- The Company offers controlled account deposit methods (virtual account numbers and card funding)

The Company does not offer any type of digital assets deposits; this eliminates the risk of the Service being used for smurfing purposes;

- The Company only accepts payments via bank transfers or cards using secured 3D payment gateways (limiting the risk of funds being placed from fraudulent sources).

However, the Service remains vulnerable to certain ML/FT attempts, including:

- Placement: introducing illicit funds into the system –it may involve splitting funds using provided virtual account number(s);

- Terrorism financing: Creating multiple accounts for the sole purpose of receiving and sending to finance terrorist-related activities

Customer Due Diligence

Given the nature of the services, to carry out proper customer due diligence, Coinplug will implement policies and procedures in its Lines of Business (LOBs), recognizing and validating the customer's identity using the following "Know Your Customer" principles:

- The identification and verification of the Customer's identity and, where applicable, the Ultimate Beneficial owners (herein after the "UBO"); and;
- Information on the donors, businesses, vendors, beneficiaries, and customers that was gathered from dependable and impartial sources ("Identity verification").

Customers (donors, businesses vendors, and users) who are classified as Listed Companies or Public Authorities and who, as a result of their regulated activities, present a lower risk of engaging in money laundering and terrorist

activity can typically benefit from the implementation of a streamlined customer due diligence process thanks to Coinplug's AML/CFT processes and procedures.

Customers who are Small and Medium–sized Businesses (SMB), which could not be Listed Companies, and those who use Coinplug will be subject to further checks and due diligence. In the same vein, an individual who uses Coinplug at any levels will be subject to further checks and due diligence.

If there is any suspicious activity throughout the customer engagement or due diligence process, it should be reported right away to the designated support contact Support@coinplug.Ng

Risk-Based Approach

Compliance with these obligations is modulated according to a risk-based approach, based on the Risk Assessment and Risk Scoring of the Customer. According to Coinplug, a customer's country of residence or the type of activities they engage in directly influences their likelihood of becoming involved in money laundering and terrorist funding schemes.

Coinplug will group its customers according to their risk level using the pertinent line of business processes and procedures. The identification of potential risks will aid in successful risk management by implementing measures to lower any recognized risks.

Changes in a User's circumstances like the ones listed below may be viewed suspiciously.

- Unusual transactions that are inconsistent with the customer's recognized business activities;
- A sudden rise in business activities from an existing Customer;
- Peak periods of activity at specific times or locations;
- Having multiple accounts with large funds from unverifiable source(s);
- Unfamiliar or untypical types of customers or transaction;

- Situations where the source of funds cannot be easily verified;
- Complex transactions and unusual transactional patterns with no discernable economic or legal reason;
- Funds sent or received from regions with a history of terrorism or high levels of crime.
-

Customer KYC

Preventing financial fraud, money laundering, financing of terrorism, and other forms of identity theft is crucial to the functioning of Coinplug. As a result, we have put in place a stringent Know Your Customer (KYC) procedure that complies with international best practices. In addition, we keep up the KYC procedure with our customers once a good working relationship has been established. Since we expect customers to update their contact an d identification details whenever they change.

Customers must use one of the following forms of formal identification:

a. Valid Government Issued Means of Identification for individuals
b. BVN Submission
c. Recent Utility Bill

Also, through our partners we can identify customers:

a. Name
b. Date of birth
c. Age
d. Nationality
e. Occupation
f. Gender
g. Address.

Enhanced Due Diligence (EDD)

The appropriate Personnel conducts an EDD of particularly complex, unusually large, not economically justified, inconsistent with the information provided or suspected of being illegal transactions, being specified that the Service does not allow particularly complex transactions to be carried out.

Whenever there is cause for suspicion, the Customer will be required to

identify and validate the source and purpose of the transactions, whether they are done by individuals or by corporations with beneficial owners. If there are no grounds for suspicion, no action is necessary.

High-Risk Customers

Coinplug will not do business with the following segments of customers:

- Persons included in any official lists of sanctions;
- Persons indicating possible involvement in criminal activities, based on available information about them;
- Persons with businesses in which the legitimacy of activity or source of funds cannot be reasonably verified;
- Persons refusing to provide the required information or documentation; or
- Entities whose shareholder/control structure cannot be determined.
- Politically Exposed Persons (PEPs)

Politically Exposed Persons(PEPs)

PEPs are people designated by their governments to perform a public obligation on their behalf. They may so represent high-risk customers because they have been given access to substantial public monies. Furthermore, they may engage in corrupt activities that have ties to AML and CFT due to their position of authority.

PEPs can be (but are not limited to the following):

a. Senior Officials in Governmental Positions
b. Ministry Appointed Positions
c. Politicians
d. Family members/Close friends of the aforementioned
e. Senior Military Officials

COINPLUG will make sure that the COINPLUG account(s) where these monies are deposited are immediately restricted limiting every form of account transactions if any suspicious transactions are detected as linked to PEP with the assistance of our partners. Therefore, we rely largely on the assistance of Banks and any

of our partners to report any suspicious activity. To prevent PEPs from participating in a transaction, we also abide by local and international regulations. We have therefore put in place various measures such as:

a. Setting transaction limits

b. Recordkeeping

c. KYC procedures

d. Flagging inconsistent IP addresses and transactions

Enhanced Due Diligence (EDD)procedure

In case of unusual or suspicious Transactions as defined herein, the Company shall obtain information from the Customer on the origin of the funds and the purpose of the Transaction:

- By sending the Customer are quest to this effect; and

- By collecting any information and documents that can justify and explain the nature of the transaction;.

To determine the risk of ML/FT and ,where appropriate, to ensure that any doubts can be legitimately ruled out, the Company shall take into account the analysis of IP addresses linked to the account of the Customer and, in particular:

- The consistency between the IP address and the characteristics of the Customer: different location of the place of residence, more than 5 different IP addresses over 30days, use of the same IP address by different Customers;

- The consistency between the activity declared by a Customer and the Transactions carried out through the Services;

- the publicly known information: individuals or entities who have been identified, including in the press, as having traveled to, attempted to, or intended to travel to high-risk countries or as being linked or potentially inked to a terrorist organization or terrorist activities;

- The information provided by the Customer: for instance, when a Customer expresses support for a terrorist organization or shows signs of violence or radicalization.

- If the information and documents provided by the Customer appear to

be sufficiently accurate and reliable to dispel any doubt as to the origin and destination of the funds, the Company shall remove account restriction.

- If not, especially if the Customer has not provided any information or provided any documents, a suspicious activity report is sent to NFIU under the conditions set out in Section 7 of the Money Laundering (Prevention and Prohibition)Act, 2022 and the Risk Scoring of the Customer is updated by the MLCO.
- In all cases the nature of the Transaction, the documents, and information collected as part of the EDD and, where applicable, the SAR, are included in the EDD File of the Customer.

Suspicious activity reports(SAR),Reporting conditions, and Reporting cases.

A suspicious activity report ("SAR") must be sent to NFIU:

Where a transaction—

(a) Involves a frequency that is unjustifiable or unreasonable,

(b) Is surrounded by conditions of unusual or unjustified complexity,

(c) Is from an unverifiable/suspicious source,

(d) Appears to have no economic justification or lawful objective,

(e) Is inconsistent with the known transaction pattern of the account or business relationship ,or

(f) In the opinion of the financial institution or non-financial business and profession involves the proceeds of criminal activity, unlawful act, money laundering or terrorist financing,

Freezing measures

— **(1)**Upon publication of the Unconsolidated List of persons and entities designated under UNSCRs that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction, all natural land, legal persons in Nigeria, including financial institutions, designated non-financial businesses and professions, and other entities in Nigeria shall be required to, immediately, identify and freeze all funds, assets, and any other economic resources belonging to a designated person or entity in their possession and

report same to the Nigeria Sanctions Committee.

— **(2)**The freezing obligation under subsection(1),shall extend to—

(a) allfundsorotherassetsthatareownedorcontrolledbythedesignatedpersonorentity,andnotjustthosethatcanbetiedtoaparticularact,plot,orthreatofproliferation;

(b) thosefundsorotherassetsthatarewhollyorjointlyownedorcontrolled,directlyorindirectly,bydesignatedpersonsorentities;

(c) thefundsorotherassetsderivedorgeneratedfromfundsorotherassetsownedorcontrolleddirectlyorindirectlybydesignatedpersonsorentities;and

(d) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

In the event of an attempt or suspicion to commit an offense punishable by a prison sentence of more than one year of there is a suspicion of money laundering or terrorist financing following the analysis of the alert detected, forward reports of suspicious transactions relating to terrorism or terrorism financing, or proliferation financing to the NFIU, which shall immediately process and forward the information to the relevant agency, where there are sufficient reasons to suspect that the funds—

(a) Are derived from legal or illegal sources, and are intended to be used for an act of terrorism or terrorism financing, or proliferation financing
(b) Are proceeds of a crime related to terrorism or terrorism financing, proliferation financing; or
(c) Belong to a person, entity, or organization considered a terrorist.

Coinplug is not liable for the violation of the confidentiality rules for any lawful action taken in furtherance of its obligations under subsection (1).

Record Keeping

— (1)Subject to the provisions of the Money Laundering(Prevention and Prohibition)Act, a financial institution or designated non-financial institution shall, within 24 hours, forward reports of suspicious transactions relating to terrorism or terrorism financing, or proliferation financing to the NFIU, which shall immediately process and forward the information to the relevant agency, where there are sufficient reasons to suspect that the funds—

(a) Are derived from legal or illegal sources, and are intended to be used for an act of terrorism or terrorism financing, or proliferation financing;

Reporting Procedures

Coinplug expects that, if any employee, contractor, or business partner becomes aware of any suspicion or knowledge of possible AML/CFT activity, this is to be reported without undue delay to our designated support, Support@coinplug.ng

The following details, which will be verified, should be included at the very least in a report on suspicious activity:

- Identity of the person raising the suspicion;
- Date of the report;
- Who is suspected of money laundering or terrorist financing activities;
- Other individuals involved otherwise;
- Deliverance of facts;
- What is suspected and why;
- Any possible involvement of Coinplug and limiting such involvement.

We may make reasonable inquiries within the Coinplug ecosystem to confirm these suspicions or obtain additional information to confirm these suspicions. Details of internal reports will be held separately, and excluded from customer files, to avoid inadvertent or inappropriate disclosure.

Reporting Officer.

The MLRO is the sole decision-maker and the only person authorized to file a SAR. In urgent cases, and if the MLRO is unavailable, any Officer or, failing that, any employee of the Company trained according to an emergency procedure, may take the initiative to report suspicions when the analysis of the Alert justifies it.

Customer information will be electronically kept. It is necessary to keep an appropriate record of the paper work that has been received, the actions that have been taken, and copies or references to the customers' documents. Records will be kept for the duration of the connection with the customer and a minimum of five (5) years after the relationship ends, incompliance with section 8 of the Money Laundering (Prevention and Prohibition) Act,2022.In countries where this duration exceeds the allowed time limit, the legally required time frame will be taken into account to comply with local laws.

DISCLAIMER. In the event any Customer is the subject of a SAR to NFIU, no civil or criminal liability may be imposed on the Company or any of its employees when the SAR was made in good faith. In the event of damage resulting directly from such a SAR or disclosure, the National Authority or Agency shall be liable for the damage suffered. These provisions shall also apply where the SAR has not be enacted upon or in the case of are part of a transaction already executed.

Content of the report.

The SAR includes the following information:

- The profession exercised by the person making the report ,i.e. provider of the services
- The identification details and professional contact details of the MLRO;
- The identification details of the Customer and, where applicable, of the beneficial owner of the Transaction that is the subject of the report and the purpose and nature of the Business relationship;
- The reason for reporting, namely: suspicion linked to offences punishable by more than one year's imprisonment; suspicion linked to the financing of terrorism; suspicion of tax fraud; suspicion following an EDD; attempted money laundering or financing of terrorism, supplementary report;
- A description of the Transaction and the elements of analysis that led to the report;
- Where the transaction has not yet been executed ,the execution deadline.

Where applicable, the SAR shall be accompanied by any other document that may be useful to NFIU

Suspension of the operations.

If the Company holds funds in legal tender on behalf of the Customer at the time of reporting, the Company must suspend the execution of any Transaction in order to allow NFIU to exercise its right of opposition until the execution deadline .In this case:

Either NFIU does not object to the transfer of funds; in this case, the Customer's Transaction can be carried out again;

- or NFIU notifies its opposition to the execution of a transaction to transfer funds to an account designated by the Customer; in this case:

- The said funds are blocked for a further period often (10) days from the date of this notification or until receipt of a No- objection from the NFIU or applicable restricting authority.

Transaction Recording and Limits

For every successful system transaction, Coinplug will record the following transaction information:

a. Source Account Information
b. Receiving Account Information
c. Transaction Reference
d. Transaction Amount
e. Transaction Date
f. A System Generated Alpha Numeric Unique Transaction Identification Token
g. Success or Failure Response Code for Transaction
h. I.P Address of the Originating Device of the Transaction
i. Transaction Time

POLICY REVIEW AND AUDITS

This Policy's efficacy is continually assessed. This provides Senior Executive management with the necessary assurance and information regarding the efficiency of Coinplug's controls and processes relevant to this Policy.

TRAINING

Partners and employees alike will receive training on their responsibilities regarding Anti-money laundering regulations so they are aware of how to identify and manage transactions that may involve money laundering. They will go through AML training every year that is tailored to the specific organizational functions they each have.

REAL-TIME TRANSACTION MONITORING AGENT

ransactions and recognizes potentially suspicious transactions using predefined criteria and scenarios. As soon as a suspicious transaction is discovered, emails and alerts are forwarded to the MLRO and management team. The alerts are examined in accorAll transactions are kept track of by a centralized monitoring system(Real-Time Artificial Intelligence Monitoring Agent/Officer),which employs cutting-edge Artificial Intelligence and Machine Learning algorithms in real-time.

The system recognizes high-risk tdance with the discovered rule. The alerts are looked in to using the AML standards under which the transaction was found. If necessary, the issue would be resolved or escalated to include other pertinent parties.

COMPLIANCEMONITORINGANDMANAGEMENT

The following processes will be routinely observed by the MLRO to make sure they are carried out incompliance with the Company's AML policies and procedures:

- Customer identity verification;
- reporting suspicious transactions;
- Record keeping.

The Management group will also monitor any adjustments and requirements put forward by the supervisory authority overseeing the Money Laundering Report. The company's AML policies and procedures will be modified as needed to achieve compliance.

STATEMENT OF INTENT

In order to fully comply with the local, relevant international laws, and the Money Laundering (Prevention and Prohibition) Act, 2022,including that anti-corruption and those banning terrorist funding, all Coinplug employees, contractors, and business partners are obliged to adhere to this policy.

VIOLATION

Any breach of this agreement, whether deliberate or unintentional, needs to be reported to the Chief Executive Officer to be escalated to the Board of Director .Any violation of the values mentioned in this document or any of the sections that are related to it will be viewed as a violation of company policy.