Anti-Money Laundering and Countering the Financing of Terrorism Policy

1. Introduction

Bramp Africa Limited (the "Company") is a private company limited by shares registered under the laws of the Federal Republic of Nigeria that provides digital products and
services.
.

This Policy serves as a comprehensive guide for the employees, management, and partners of the Company to establish measures that prevent it from being used as a channel for money laundering activities. Its primary objective is to equip the staff and management with essential knowledge about the Company's anti-money laundering and counter-terrorism financing (AML/CFT) prevention framework, thereby reducing the risks associated with such illegal activities.

The Company is fully dedicated to upholding compliance with all relevant local and international laws, regulations, and standards mandated by authorities concerning the prevention of money laundering and terrorist financing.

2. Scope of the Policy

The broad definition of money laundering means that potentially anyone could commit a money laundering offence, and this includes all employees of the Company.

Our Policy is to enable the Company to meet its legal and regulatory requirements in a way which is proportionate to the risk nature of the business, by taking reasonable steps to minimise the likelihood of money laundering occurring.

All employees must be familiar with their legal responsibilities and failure to comply with this Policy may lead to disciplinary action.

As a result, the employees of the Company shall be vigilant for any suspicious activity and report it immediately to the compliance officer for immediate reporting to

the Nigerian Financial Intelligence Unit (the NFIU) of the Economic and Financial Crimes Commission (EFCC), in accordance with specified policies and procedures, so that they may in turn notify the relevant authorities. Only through the commitment of the management and the employees of the Company shall it be possible to guarantee that the products and services of the Company cannot be used for money laundering or financing of terrorism acts.

Adherence to this Policy is absolutely fundamental to ensuring that the Company comply fully with anti-money laundering and terrorism financing legislations. Employees are required to be actively involved in the implementation and development of this Policy.

3. What is Money Laundering and Terrorism Financing?

The relevant legislations are the Money Laundering (Prevention and Prohibition) Act, 2022, the Terrorism (Prevention and Prohibition) Act 2022, the Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing of Weapons of Mass Destruction in Financial Institutions Regulations, 2022, and the National Insurance Commission Anti-Money Laundering and Combating the Financing of Terrorism (NAICOM AML/CFT) Regulations 2013.

Money laundering can be defined as the process to move illegally acquired cash through financial systems so that it appears to be from a legitimate source. Money laundering offences include: participation in an organised criminal group or racketeering; terrorism, including terrorism financing; financing the proliferation of weapons of mass destruction; bribery; corruption; fraud; etc.

Terrorism financing is defined as the providing, depositing, distribution or collecting of funds, by any means, directly or indirectly, intended to be used, or knowing that they are to be wholly or partially used, for the committing of terrorist acts.

There are also several secondary offences, such as failure to disclose knowledge or suspicion of money laundering to the Compliance Officer (CO); failure by the CO to disclose knowledge or suspicion of money laundering to the Nigerian Financial

Intelligence Unit; and 'tipping off' whereby somebody informs a person or persons who are, or who are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation.

Any member of staff could potentially be caught by the money laundering provisions, if they suspect money laundering and either become involved with it in some way, and/or do nothing about it. This Policy sets out how any concerns should be raised.

4. **Anti-money laundering Compliance Officer (AML CO)**

The Company will appoint a CO to receive disclosures about money laundering activity and be responsible for anti-money laundering activity within the Company. The officer nominated to do this is [Aloaye Daniel].

The CO will ensure that appropriate training and awareness is provided to new and existing employees of the Company and that this is reviewed and updated as required.

The CO will ensure that appropriate anti-money laundering systems and processes are incorporated by the Company.

5. Customer Acceptance Policy

5.1. Business risk evaluation and management

The Company considers that the potential threat of becoming involved in any money laundering or terrorism activity is directly related to the type of business carried out by the Company and that such threat can be more effectively and efficiently managed if the potential risk linked to the business and products of the Company is known before.

Classifying its products by risk levels shall enable the Company to design and implement measures and controls to mitigate such risk. Likewise, it shall enable the Company to focus on those business lines and products that present greater risk. Therefore, the Company shall apply a procedure that shall enable them to determine the risk of the business lines in which they participate and the products they distribute, with respect to money laundering

or terrorism financing. The criteria and factors to be used for measuring such potential risk should also be identified.

In the same sense, risks inherent in money laundering or terrorism financing can be managed more effectively and efficiently if the potential risk linked to the different types of customers and their transactions is known beforehand.

Having customers and their transactions identified by risk level shall enable the Company to design and implement measures and controls to mitigate such risk. Likewise, it shall enable them to focus on those customers and transactions that present the greatest risk. In peculiar cases, such risk may only become apparent over time, such concerns thus make it prudent to monitor and/or report such customer's policies and activities as a fundamental component of our risk-based approach.

In this sense, the Company shall design a procedure, based on the risk consideration of their own business and the products marketed by them, which shall provide an appropriate framework for segmenting their own customers by levels of money laundering or terrorism financing risk. The criteria and factors to be used for making such segmentation should also be identified.

5.2. Assessing risks and applying a risk-based approach

In compliance with the international standards on countering money laundering and the financing of terrorism & proliferation based on FATF Recommendation 1, the Company shall apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The Company shall adopt a risk-based approach in respect of profiling AML/CFT along the following lines:

a. Client;
b. Geographies;
c. Product & services; and
d. Distribution channels.

5.3. Prohibited customers or with reinforced acceptance measures

For money-laundering and terrorism financing risk control purposes, the Company shall not accept the following categories of customers:

a. Persons included in any of the official lists of sanctions ("applicable lists"). e.g United Nations Security Council (UNSC) Sanctions List.
b. Persons about whom information is available indicating possible involvement in criminal activities.
c. Persons with businesses that make it impossible to verify the legitimacy of their activities or the source of funds.
d. Persons who refuse to provide the required information or documentation.
e. Legal entities whose shareholder or control structure cannot be determined.
f. Casinos or gambling/betting establishments that are not officially authorized.
g. Financial institutions resident in countries or territories without being physically present (also referred to as "shell companies") and which do not belong to a regulated financial group.

Clients classified as Political Exposed Persons (PEPs) shall only be accepted as customers with prior authorization from any member of senior management in line with regulation 9(7) of the NAICOM AML/CFT 2013.

Political Exposed Persons (PEPs) - Customers who are high-level public officials and their family members, and well-known personalities wishing to purchase insurance products outside their native countries.

5.4. Know-Your-Customer (KYC)

The most effective means of preventing the use of the financial system for money laundering or terrorism financing is to identify and know your customers, regardless of whether they are established customers or otherwise.

Along these lines, the Company shall establish regulations, procedures, and internal controls aimed at obtaining effective and complete knowledge of their customers and their activities, in order to:

a. Confirm and document the true identity of customers who maintain any type of insurance service relationship.
b. Confirm and document any additional customer information commensurate with the assessment of the money laundering and terrorism financing risk.
c. Ensure that the Company does not engage in business with any individuals or entities whose identities cannot be confirmed, who do not provide all required information, or who have provided information that is false or that contains significant inconsistencies that cannot be clarified.

For customer identification, the Company shall consider the following criteria:

a. In the case of individuals, an official identification document shall be required to confirm the individual's identity.
b. For corporations and other legal entities, the documents of incorporation must be presented, including information concerning the customer's name, legal form, address, directors, and the corporate bylaws, powers of attorney, entry in the appropriate register or other reliable identifying information.
c. Neither anonymous accounts nor accounts using fictitious names may be opened or maintained.

In these cases, all requirements must be fulfilled, including identification of the beneficial owner of the account, in accordance with the provisions of established AML/CFT regulations.

The Company shall have procedures for determining that person's identity and relationship to the customer. All necessary measures shall be taken to obtain information about the true identity of the person on whose behalf a relationship is established, the insurance product, or a significant transaction conducted (that is, the beneficial owners) whenever the customer is acting on behalf of third parties or in cases where doubts exist as to whether the customer is acting on its own behalf.

6. **Suspicions of Money Laundering**

All employees must immediately and as soon as possible report any knowledge of or suspicion of (or where there are reasonable grounds to suspect) suspicious activity to the CO in the prescribed form as set out in this policy document.

Once the matter has been reported to the CO, the employee must follow the directions given to him/her and must NOT make any further enquiry into the matter.

The employee must NOT voice any suspicions to the person(s) whom they suspect of money laundering, as this may result in the commission of the offence of “tipping off”. They must NOT discuss the matter with others or note on the file that a report has been made to the CO in case this results in the suspect becoming aware of the situation.

7. **Consideration of the Disclosure by the CO**

Once the CO has received the report, it must be evaluated in a timely manner in order to determine whether:

- There is actual or suspected money laundering taking place; or
- There are reasonable grounds to know or suspect that this is the case; and
- Whether the CO needs to lodge a Suspicious Activity Report (SAR) with the NFIU.

Where the CO concludes that there are no reasonable grounds to suspect money laundering, then consent will be given for any on-going or imminent transaction(s) to proceed.

Where consent is required from the NFIU for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the NFIU has given specific consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NFIU.

All disclosure reports referred to the CO and reports made to the NFIU will be retained by the CO in a confidential file kept for that purpose, for a minimum of 5 years.

The CO must also consider whether additional notifications and reports to other relevant enforcement agencies should be made.

8. Customer Identification and Due Diligence

Due diligence is performed on all customers of the Company who must provide basic information including full name, residential/business address, date of birth, and registration details for corporate bodies.

8.1. Enhanced Due Diligence

It may be necessary for the Company to carry out enhanced due diligence on certain customers where the customer or a transaction involving the customer appears to be “high risk”. This means that there is a higher level of identification and verification of the customer’s identity required. The following non-exhaustive list of situations may indicate a “high risk”:

- a new customer;
- a customer not well known to the Company;
- customers in known high risk industries and/or jurisdictions;
- transactions that are unusual or appear to be unusual for that customer;
- highly complex transaction or payment arrangements;
- companies that have nominee-shareholders or shares in bearer form;

- legal persons or legal arrangements such as trusts that are personal assets-holding vehicles;
- cross-border and banking and business relationships;
- the transaction involves a politically exposed person ("PEP") or an immediate family member or a close associate of a PEP; and
- no face-to-face meetings take place with the customer where this is usually expected.

Employees must assess the money laundering risk for each customer and if you suspect enhanced due diligence is required, you should speak to the CO before continuing any engagement with the customer. The CO will be required to approve the continuance of the Company's business relationship with such customers.

If enhanced due diligence is carried out, the CO must:

- obtain additional information on the customer and on the customer's beneficial owner(s);
- obtain additional information on the intended nature of the business relationship;
- obtain information on the source of funds and source of wealth of the customer and customer's beneficial owner(s); and
- conduct enhanced monitoring of the business relationship.

This may include but is not limited to the following:

- checking the organisation's website to confirm the identity of personnel, its business address and any other details;
- attending to the customer at their business address;
- obtaining additional information or evidence to establish the identity of the customer and its beneficial owner(s), including checking publicly available beneficial ownership registers of legal entities such as the registers available at the Corporate Affairs Commission;
- in the case of a PEP, seek the approval of senior management and establish the source of wealth and source of funds; and

- ensure that the first payment is made into a bank account in the customer's name.

If satisfactory evidence of identity is not obtained at the outset, then the business relationship or one-off transaction(s) cannot proceed any further. A report should be filed with the CO who will then consider if a report needs to be submitted to the NFIU.

9. Reporting Obligations

9.1. Criminal Activity

Where the Company reasonably suspects that the source of funds is the proceeds of criminal activity, it shall report its suspicion to the NFIU Immediately and all suspicious transactions including attempted transactions shall be reported regardless of the amount involved and the report shall include any action taken on the suspicious activity.

9.2. Terrorism Links

Where the Company reasonably suspects that a transaction is linked with terrorism, it shall report its suspicion to NFIU Immediately and without delay but not later than 24 (twenty-four) hours.

Similarly, it shall amount to reasonable suspicion, where the Company has reasonable grounds to suspect that the funds in question:

a. Are intended to be used for an act of terrorism notwithstanding that such funds derive from legal or illegal sources;

b. Are proceeds of a crime related to terrorism financing; and

c. Belong to a person, entity or organization considered a terrorist.

9.3. Currency Transactions Reporting

Currency Transaction Reporting (CTR) timeline: immediately but not later than 7 (seven) days of occurrence.

The Company is under obligation to file all Currency Transaction Reports (CTRs) above the statutory threshold to the NFIU:

a. Any payment from ₦5,000,000 (five million Naira) or its equivalent in foreign currency in the case of an individual.
b. Any payment from ₦10,000,000 (ten million Naira) or its equivalent in foreign currency in the case of a corporate entity.
c. Any payment or transfer from/to a foreign country of funds exceeding $10,000,000.00 (ten million Dollars).

Where there are no instances of suspicious and currency transactions, the Company shall file a NIL report for industry regulatory compliance purposes.

10. Ongoing Monitoring

Employees should review customers at regular intervals to ensure that the risk level of each customer's information and information held on each customer is not only accurate and up to date, but is consistent with the knowledge of the customer and its business. Further due diligence may be required if new people become involved as a customer. Any suspicious activity must be reported to the CO.

11. Data Protection

Customer details must be collected in accordance with the Nigeria Data Protection Regulation 2019 and the Nigerian Data Protection Act 2023. This data can be "processed" as defined under the Nigeria Data Protection Regulation 2019 to prevent money laundering and terrorist financing.

12. Record Keeping

Customer identification evidence and details of any relevant transaction(s) for that customer must be retained for at least 5 (five) years from the end of any business relationship with that customer.

13. Staff

In compliance with the provisions of the NAICOM AML/CFT Regulations 2013, the Training unit shall facilitate training programs that shall make employees and agents to be fully aware of their obligations e.g. identifying suspicious transactions and equip them with the relevant skill required for the effective discharge of their AML/CFT tasks.

The Company shall adopt any of the following staff training methods;

a. Classroom training;
b. Electronic learning management systems (ELMS);
c. Email Communication broadcast to all Staff on AML/CFT subject matter; or
d. Mandatory company-wide Knowledge sharing sessions

The training programs shall consider international standards and local legislation to prevent money laundering and terrorism financing, the latest trends in criminal activity, and the Company's policies and procedures designed to counter money laundering and terrorism financing, including how to recognize and report suspicious activities.

A specific record shall be kept of all training activity given, stating the date, place and duration of each course, the number of attendees and the Unit to which they belong

14. Implementation of Policy

This Policy shall be deemed effective as of [30/04/2025]. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

…….
Chibuike Emmanuel Nwogbo
Chief Executive Officer

Approved by:		Version:	1.0
Responsible official:	Aloaye Daniel	Effective date:	30/04/2025

Revision history

Version	Effective date	Approved by	Summary of changes
1.0	30/04/2025	Chibuike Nwogbo	NA

CONFIDENTIAL

Report to the Anti-money laundering Compliance Officer

Report of Money Laundering Activity

To: **Anti-money laundering Compliance Officer**

From: _____

[Insert name of employee**]**

Title: _____

[Insert Title**]**

Tel No: _____

URGENT YES/NO

Date by which response needed: _____

Details of suspected offence:

Name(s) and address(s) of person(s) involved:

[If a company, please include details of nature of business**]**

Nature, value and timing of activity involved:

[Please include full details e.g. what, when, where, how. Continue on a separate sheet if necessary**]**

Nature of suspicions regarding such activity

[Please continue on a separate sheet if necessary**]**

[Please attach any supporting documentation that may be relevant**]**

Has any investigation been undertaken (as far as you are aware)?
Yes / No

If yes, please include details below:

Have you discussed your suspicions with anyone else? YES/NO

If yes, please specify below, explaining why such discussion was necessary:

Please set out below any other information you feel is relevant:

Signed: _____ Dated: _____

Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a 'tipping off' offence, which carries a maximum penalty of 5 years' imprisonment.

THE FOLLOWING PART OF THIS FORM TO BE COMPLETED BY THE CO

Date report received: _____

Date receipt of from acknowledged: _____

CONSIDERATION OF DISCLOSURE:

Action plan:

OUTCOME OF CONSIDERATION OF DISCLOSURE:

Are there reasonable grounds for suspecting money laundering activity?

If there are reasonable grounds for suspicion, will a report be made to the NFIU?

Yes/No

If yes, please confirm date of report to the NFIU: and complete the box below.

Details of liaison with the NFIU regarding the report:

Notice Period: from: to:

Moratorium Period: from: to:

Is consent required from the NFIU to any ongoing or imminent transactions, which would otherwise be prohibited acts?

Yes/No

If yes, please confirm full details below:

Date consent received from the NFIU:

Date consent given by you to employee:

If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to the NFIU, please set out below the reason(s) for non-disclosure:

[Please set out any reasonable excuse for non-disclosure**]**

Date consent given by you to employee for any prohibited act transactions to proceed:

Other relevant information:

Signed: _____ Dated: _____

THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS

The above document was given to …… to familiarise him/herself with its contents and the actions required by him/her and the company should the need arise.

He/She has understood and been tested on the contents of the company's anti money laundering policy document and shows a thorough understanding of his/her responsibilities with regard to that document.

Signed…….. …….. – Director

Signed …… …….. - Employee

Date ……