



PRINCEPS CREDIT SYSTEMS LIMITED

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY



DOCUMENT INFORMATION

Version	Date	Owner(s)	Author	Description	Effective Date
1.0	April 2025	People and Culture; Finance; Legal and Compliance	Ekene Ugbede	Creation	June 2, 2025

REVIEWED BY

S/No	Name	Designation	Signature	Date
1.	Naomi Okpalo	Head, People and Culture		April 15, 2025
2.	Oluwatoyosi Adetula	COO/Executive Director		April 15, 2025

APPROVED BY

S/No	Name	Designation	Signature	Date
1.	Oluwatoyosi Adetula	COO/Executive Director		May 15, 2025
2.	Peter Atuma	Executive Chairman		May 15, 2025

1. POLICY STATEMENT

- 1.1 As a company, we intend to carry on business in accordance with all applicable laws, the highest ethical standards and international best practices. These include applicable laws aimed at combating money laundering and terrorism financing.
- 1.2 We say a firm **No** to money laundering and terrorism financing. We intend to conduct business with customers, service providers and other parties who are only involved in legitimate business activities and whose funds are solely derived from or traceable to legitimate activities and sources.
- 1.3 This policy outlines our respective roles and simultaneously provides a framework for the prevention, identification and disclosure of any potential, suspected or actual threat of money laundering and terrorist financing.

2. WHO IS COVERED BY THIS POLICY?

- 2.1 This policy applies to all employees, directors, officers, and staff of the company (whether permanent, fixed-term or temporary; associates, trainees, agency staff, seconded staff, homeworkers, volunteers, interns, agents). It also applies to all external stakeholders - customers, consultants, contractors, service providers, vendors, suppliers and business partners of the company; and all other persons and entities who may engage with the company in any respect.

3. EXPOSURES

An adherence to this policy is crucial. A violation may expose the company and relevant persons to severe legal, financial, commercial and reputational risks. These include the risk of severe regulatory sanctions, fines, imprisonment, and lengthy investigations, amongst others.

4. MONEY LAUNDERING AND TERRORIST FINANCING

- 4.1 Money laundering is the process of concealing, disguising, integrating or exchanging monies or assets that were obtained from criminal activities (“criminal property”) for monies or assets that are clean. Money laundering seeks to hide the link or source of criminal property so there is no visible link to their criminal sources. Criminal property may be tangible or intangible.
- 4.2 Terrorism financing involves raising, depositing, circulating, collecting or processing funds, knowing that such funds are to be applied towards committing acts of terrorism.
- 4.3 Our company does not intend to deal with any person or entity that has been identified by any relevant authority as potentially linked to terrorist activities in Nigeria or in any other jurisdiction.
- 4.4 A violation of this policy may occur where any person covered by this policy is aware of or reasonably suspects the existence of any criminal property and permits the conduct of any business in respect of such property without making a report.

4.5 No person covered by this policy is permitted to:

- a. engage in any form of money laundering or terrorism funding.
- b. knowingly permit any entity or individual to use our company as a conduit for money laundering or terrorism financing activities.

4.6 Where you have reasons to suspect the existence of any criminal property or that a criminal act has taken place or is likely to take place, you should consider whether there is a risk that money laundering or terrorist financing has occurred or may occur and make a report to your line manager, supervisor, the Legal Department, or the compliance officers, in that regard.

5. **ANTI-MONEY LAUNDERING AND COUNTERING OF TERRORISM-FINANCING PROCEDURE**

5.1 To the extent practicable, no person covered by this policy shall establish a relationship with or conduct a transaction with any person:

- 5.1.1 Whose identity or legitimacy cannot be satisfactorily determined.
- 5.1.2 Who fails to provide any information necessary for complying with this policy;
- 5.1.3 Who has provided any such information which contains obvious or material inconsistencies or inaccuracies which could not be satisfactorily resolved after an investigation; and
- 5.1.4 Whose funds appear to be the proceeds of an illegal activity, or who is involved in or intends to apply any part of the funds towards an illegal activity.

6. **RED FLAGS**

6.1 The following is a non-exclusive list of potential red flags that may indicate suspicious transactions or activities:

- (a) A person provides insufficient, unusual, suspicious or false information; or is reluctant to provide complete information; or provides information that cannot be easily verified;
- (b) Methods of payment that are inconsistent with our payment requirements or which may appear to be unusual e.g. payments by money orders, traveller's checks, multiple instruments, or unrelated third parties.
- (c) Payment in cash or a request to pay in cash, unless where necessary.
- (d) Premature or unusual repayments, especially where such payment is from an unrelated third party or involves an unusual form of payment.
- (e) Payments to or from third parties that have no visible or reasonable connection with a party or transaction.
- (f) Payments to or from countries unrelated to the transaction or which do not appear to be

logical.

- (g) Payment to or from countries considered tax havens; offshore jurisdictions, or countries considered to be high risk for money laundering or terrorist financing activities.
- (h) Any business whose registration documents are from a tax haven, or a country that poses a highrisk for money laundering, terrorism or terrorist financing.
- (i) Overpayments followed by directions to refund any payment either directly or to a third party.
- (j) Unusually complex business structures and payment patterns that reflect no real business purpose.
- (k) Transactions which are unusual or not consistent with the business patterns, activities or economic profile of such party.
- (l) Transactions which, by their very nature, may be associated with money laundering.
- (m) Any other activity or deviation from any usual or accepted business practice, that could occasion a red flag.

7. PROCESSES AND CONTROLS

7.1 There shall be:

- 7.1.1 A continuous risk management and due diligence process to verify, assess and profile customers, service providers and other parties according to their risk exposure.
- 7.1.2 Proper record-keeping of customer, agents and service providers transactions, detection and identification checks, and suspicious activity reports.
- 7.1.3 Periodic training for all relevant employees on their relevant responsibilities.
- 7.1.4 Regular audit and testing of relevant controls, to ascertain their effectiveness and identify areas that require improvement, with relevant reports being made to senior management and the board of directors.

7.2 KNOW YOUR CUSTOMER (KYC)

- 7.3 Where practicable and to the extent possible, we aim to carry out due diligence at the outset of any business relationship with any other party prior to any formal engagement.
- 7.4 The purpose of such exercise is to verify that such parties are who they say they are and to ascertain whether any visible business or legal barrier exists, prior to entering into a formal contract with them.
- 7.5 We may provide transactional limits and tiered know-your-customer monitoring where

appropriate, for transactions and activities that may be susceptible to money laundering or terrorism financing.

- 7.6 We may adopt a tier-system (e.g. tier 1, tier 2, tier 3) in relation to the risks associated with a business relationship, to reflect whether low risk, medium risk or high risk.
- 7.7 We may also obtain additional KYC information and conduct further due diligence checks on our existing service providers and any other party who we have a business relationship with, where we become aware of any red flags or otherwise.
- 7.8 The results of any such exercise will be considered in deciding whether we will do business (or continue to do business) with any such party. Relevant records must be kept as evidence of the due diligence undertaken.
- 7.9 The relevant departments and engaging or relationship officers, must regularly monitor and review the customers and service providers to identify whether any visible business activity that could indicate money laundering or terrorist financing is taking place.
- 7.10 We may establish, modify and implement any such KYC requirements or framework as we consider necessary from time to time.
- 7.11 Where we consider necessary, we may refrain from rendering any service or granting access to any service we offer (whether in full or in part), until the required KYC information has been provided. The service access and transaction limits permitted may be proportionate to the extent of KYC information obtained, where practicable.
- 7.12 We may also utilize identity checks and adopt such biometric verification measures where we consider necessary, for minimizing or mitigating risks such as unauthorised access or identity theft.
- 7.13 Relevant KYC information may include, but is not limited to:
 - (a) Full Name
 - (b) Phone number
 - (c) Passport Photo
 - (d) Valid means of identification
 - (e) Proof of address
 - (f) Date of birth
 - (g) Bank Verification Number (BVN)
 - (h) National Identification Number
 - (i) Email address
 - (j) Gender
 - (k) Religion
 - (l) Workplace
- 7.14 For organisations and entities, we may require their business or corporate registration documents detailing their current status, ownership and directorship amongst others.

8. SUSPICIOUS TRANSACTION REPORTING

- 8.1 We reserve the right to refuse to authorize, utilize, provide, process or participate in any transaction or activity where we suspect that such activity may be connected in any way to money laundering, terrorism financing or any other criminal activity.
- 8.2 All persons covered by this policy are required to report any actual or suspected case of money laundering or terrorism financing to the company.
- 8.3 In appropriate cases, we may make reports to the Nigerian Financial Intelligence Unit (NFIU). In line with the Terrorism (Prevention) Act 2011, the company will be required to report to the NFIU, within a period not more than 72 hours, any suspicious transactions relating to terrorism, where we have sufficient evidence to suspect the existence of funds linked to terrorism.
- 8.4 Upon a request or investigation by a regulatory or law enforcement agency, we will provide any relevant records related to any customer or other party who is the subject of such investigation.

9. WATCHLIST SCREENING:

- 9.1 We will refrain from engaging in any business relationship with a person who we know to be on any relevant sanction lists.
- 9.2 We will also exercise caution when dealing with politically exposed persons. That is, persons who we know have been entrusted with prominent public functions or positions.

10. EMPLOYEE RESPONSIBILITIES

- 10.1 Every employee must read and adhere to this policy; as well as any training or other relevant information provided.
- 10.2 All employees and other persons subject to this policy are responsible for the prevention, detection, and reporting of money laundering or terrorism financing red flags. They are also required to avoid any activities that could lead to, or imply, a breach of this policy.
- 10.3 If you have any reason to believe or suspect that there has been, or there is likely to be a breach of this policy, you must immediately notify your line manager, the compliance officers or the Legal Department without notifying anyone involved in the transaction.

11. SANCTIONS

- 11.1 Any employee who breaches this policy or who permits anyone to violate any provision of this policy may be subject to appropriate disciplinary action, up to and including dismissal, and may also face civil and criminal proceedings where applicable.
- 11.2 The Company shall have the right, at all times, to terminate its contractual relationship with any employee or other person who breaches this policy.

12. WHISTLEBLOWING

- 12.1 We encourage you to *Speak Up, Step Up* and raise concerns as early as possible if you observe, genuinely suspect in good faith, or have knowledge of any conduct that may violate this policy.
- 12.2 Where unsure, please speak to your line manager or the compliance officers, or the Legal and Compliance Department.
- 12.3 Concerns may also be reported by following the procedure set out in our Whistleblowing Policy. Any such reporting will be treated as confidential to the extent permitted by law and our Whistleblowing Policy. Failure to report a violation of this policy constitutes an independent violation of this policy, which may be subject to disciplinary action, and which could result in disciplinary sanctions up to and including a dismissal.

13. GENERAL PROTECTION

Rest assured that where you report a suspicious transaction or supply any information in connection with a suspicious transaction report, you will not be held liable where your suspicion is genuine and the disclosure has been made in good faith. However, this protection will not apply where it is discovered that such report is malicious in nature and false, given in bad faith or given with an intent to mislead the users of the report.

14. TRAININGS

- 14.1 We will provide relevant trainings on this policy from time to time.
- 14.2 All employees must attend all mandatory trainings organized by the company in respect of this policy.

15. RECORD-KEEPING

- 15.1 It is essential to properly keep and maintain detailed and accurate records in respect of our engagement with and transactions involving other parties.
- 15.2 Records of all registered customers and other persons covered by this policy and relevant KYC information (ID records and transaction history) must be kept for at least 6 years after any such relationship has ended, where practicable.
- 15.3 Transaction records should, where applicable and practicable, include the date and time of the transaction, amount, names of originator and beneficiary and the currency.

16. MONITORING

- 16.1 Collaboratively, the line managers, supervisors and compliance officers have the day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, and dealing with any queries on its interpretation or implementation.

- 16.2 All line managers and supervisors at all levels must ensure that those reporting to them are aware of this policy and of the crucial need for our business to be conducted in an ethical and responsible manner.
- 16.3 Each department or function could have an appointed compliance officer/assistant within it to ensure the day-to-day compliance with this policy and to circulate any relevant information across the company.
- 16.4 Surveys and audits shall be conducted from time to time on the internal control systems and procedures designed to prevent money laundering and terrorist financing to ensure their effectiveness and adequacy.
- 16.5 All employees and other persons subject to this policy are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.
- 16.6 Employees are encouraged to offer their feedback on this policy if they have any comments, suggestions or queries.
- 17. **REVIEW**
 - 17.1 We may review this policy from time to time to bring same in line with relevant legislation, best practices, improvements and advancements, and to optimise its effectiveness in achieving its objectives.
 - 17.2 We may also undertake a yearly review of this policy.