uncletimdigital@gmail.com | 08107198344
UNCLETIMTECH.COM

ANTI-MONEY LAUNDERING & COUNTERING THE FINANCING OF TERRORISM (AML/CFT) POLICY

Version 1.0 — Effective 5 November 2026 | Company: UNCLETIM DIGITAL SOLUTIONS LTD (RC 9959889), Nigeria | Product scope: UDS PAY (wallets and virtual accounts provided through 9 Payment Service Bank)

1. Policy statement

1.1 UNCLETIM DIGITAL SOLUTIONS LTD ("the Company") is committed to preventing its products from being used for money laundering, terrorist financing, proliferation financing, fraud, or other financial crime, and to complying with the Money Laundering (Prevention and Prohibition) Act 2022, the CBN AML/CFT/CPF Regulations 2022, the CBN's Baseline Standards for Automated AML Solutions (2026), and the Nigeria Data Protection Act 2023.

1.2 UDS PAY is not a bank. Customer wallets and virtual accounts are issued and held by 9 Payment Service Bank (9PSB), a licensed payment service bank, under a Wallet-as-a-Service arrangement. As the licensed institution, 9PSB carries the statutory reporting duties described in Section 8. The Company carries the duties in this Policy for the activities it performs: customer onboarding intake, tier assignment, transaction initiation, monitoring of its own platform, escalation, and evidence retention.

2. Governance

2.1 The Board/Director has overall responsibility for this Policy and approves it and any material amendment.

2.2 The Company designates a Compliance Officer responsible for the day-to-day operation of this Policy: maintaining procedures, reviewing escalations, liaising with 9PSB's compliance function, and reporting to the Director at least quarterly and immediately on any material incident.

2.3 All staff with customer-facing, operations, or engineering roles affecting onboarding, payments, or monitoring must complete AML/CFT training on joining and at least annually. Training attendance is recorded.

3. Risk-based approach

3.1 The Company applies a risk-based approach. Its principal mitigant at product level is the tiered KYC structure: transaction and balance limits rise only with the strength of verified identity (Section 4), so unverified or lightly verified customers cannot move material value.

3.2 A documented AML risk assessment of the product, channels, customer types, and geographies is maintained and reviewed at least annually and whenever the product changes materially.

4. Customer due diligence (CDD)

4.1 Tier 0 (Unverified). Registration collects name, email, username, and phone number. Limits: ₦0. No virtual account is issued and no funds can be sent.

4.2 Tier 1 (Basic Identity). Requires a Bank Verification Number (BVN) or National Identification Number (NIN), verified electronically, plus the customer's recorded consent to verification. Verification runs through 9PSB's identity service against the NIBSS/NIMC databases, including an OTP challenge to the BVN-linked phone number or a facial match option provided by that service. Limits: ₦20,000 per transaction, ₦50,000 daily, ₦300,000 maximum balance.

4.3 Tier 2 (Full Identity). Requires BVN and NIN plus a face match. Limits: ₦50,000 / ₦200,000 / ₦500,000.

4.4 Tier 3 (Enhanced). Requires Tier 2 plus a government-issued ID, proof of address, and a liveness check. Limits: ₦1,000,000 / ₦5,000,000 / no balance cap.

4.5 No account may transact above the limits of its tier; limits are enforced by the platform on every transaction, not merely displayed.

4.6 Enhanced due diligence (EDD). Customers identified as Politically Exposed Persons (PEPs), or otherwise assessed as high risk, require senior approval before Tier 2 or Tier 3 is granted, establishment of source of funds/wealth, and enhanced monitoring. The Company may decline any customer whose risk it cannot manage.

4.7 Refusal and exit. Where CDD cannot be completed, or documents/identifiers do not verify, the account remains at Tier 0 or is closed. Funds, if any, are handled per 9PSB's instructions and applicable law.

5. Screening

5.1 Accountability for sanctions, PEP, and watchlist screening of wallet customers rests with 9PSB as the licensed institution; that duty is non-delegable under the CBN AML/CFT/CPF Regulations. Screening is performed within 9PSB's identity and account-opening flow before any wallet is opened.

5.2 The Company will not open, upgrade, or knowingly operate an account for a person it knows to be a confirmed match on an applicable sanctions list, and will act immediately on any screening outcome communicated by 9PSB, including freezing activity on the platform side pending the bank's instruction.

5.3 Evidence duty. For every customer, the Company obtains and retains the screening/verification evidence available to it (identifiers submitted, verification timestamps and results, the service used, and any alert dispositions communicated to it), so that a complete per-customer file can be produced to 9PSB or a regulator on request, without delay.

5.4 Development commitment. The Company is implementing platform-side screening tooling, alert review, and case management in its compliance programme under the CBN Baseline Standards for Automated AML Solutions, aligned to the Standards' compliance horizon for other financial institutions (March 2028), with progress reviewed by the Director quarterly. Until that tooling is live, the controls in Sections 4, 6, and 7 operate and are evidenced as described.

6. Transaction monitoring

6.1 Controls operating on the platform today:

- a. Tier limits enforced per transaction and per day on every transfer;
- b. A transaction PIN, with automatic lockout after 5 consecutive failed attempts for 15 minutes;
- c. Rate limits on authentication, PIN, verification, and transfer endpoints;
- d. An immutable double-entry ledger: every movement of funds produces balanced entries, and an automated check at least hourly proves that wallet balances equal ledger sums;
- e. Automated operational monitoring of webhook anomalies, failed jobs, privilege changes, and login failures, with alerts to the operations team;
- f. Manual review of exceptions, including pending reversals and unmatched credits, through the administrative console.

6.2 Staff must escalate to the Compliance Officer any transaction or pattern that is unusual for the customer, inconsistent with their tier or profile, structured to avoid limits, or otherwise suspicious. There is no minimum amount for escalation.

6.3 Behavioural and rule-based automated transaction monitoring (typology rules, velocity analytics, anomaly detection) forms part of the development commitment in Section 5.4. Its absence today is compensated by the preventive limits in 6.1(a) and the detective controls in 6.1(d)–(f), and this position is disclosed to 9PSB as part of partnership due diligence.

7. Internal escalation and prohibition on tipping off

7.1 Any staff member who suspects money laundering or terrorist financing must report it internally to the Compliance Officer immediately, and in all cases the same business day.

7.2 No person may disclose to the customer or any third party that a suspicion has been raised, an escalation made, or a report filed ("tipping off"). Breach of this rule is a disciplinary matter and may be a criminal offence.

8. Reporting to the NFIU

8.1 Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs) for wallet accounts are filed with the Nigeria Financial Intelligence Unit through goAML by 9PSB, the licensed institution holding the accounts; goAML registration requires an operating licence, which the Company does not hold.

8.2 The Company's duty is to ensure 9PSB can meet its filing clocks (STR: immediately on forming suspicion, and in any event within 24 hours). Accordingly the Company will:

- a. Escalate every internally confirmed suspicion to 9PSB's compliance function immediately, by the fastest agreed channel;
- b. Deliver the complete customer file (CDD records, screening evidence per Section 5.3, full transaction and ledger history) without delay on request;
- c. Preserve all related records and suspend further dealing as instructed by 9PSB, subject to law.

8.3 Should the Company in future obtain a licence or designation that makes it a reporting entity in its own right, this Policy will be amended and the Company will register on goAML and file directly for its own activities.

9. Record keeping

9.1 CDD records, screening evidence, transaction and ledger records, escalation records, and training records are retained for at least five (5) years after the end of the business relationship or the date of the transaction, whichever is later, and are producible to 9PSB or a competent authority within 48 hours of a lawful request.

9.2 Records are stored with access controls and audit logging consistent with the Company's Data Protection & Privacy Policy and the NDPA.

10. Freezing and sanctions compliance

On becoming aware of a confirmed sanctions match or a direction from 9PSB, a regulator, or a court, the Company will immediately block further platform activity for the affected customer (logins, transfers, and tier changes), preserve records, and notify the Compliance Officer and 9PSB the same day. Unfreezing occurs only on written instruction from the directing authority or 9PSB.

11. Audit and review

11.1 This Policy is reviewed at least annually, on any material regulatory change, and after any material incident.

11.2 Compliance with this Policy is tested as part of the Company's information security and internal audit programme; findings are reported to the Director with remediation dates.

12. Related documents

Data Protection & Privacy Policy · Information Security Management System Policy · Risk Assessment & Incident Response Plan · Customer Complaints Policy · UDS PAY Terms & Conditions · UDS PAY Privacy Notice.

Version 1.0 — Effective 5 November 2026. Approved by: _____ (Director) · Date: _____

UNCLETIM DIGITAL SOLUTIONS LTD, RC 9959889.