AML/CFT / PROPOSED IMPLEMENTATION AMENDMENT

Madiba Verify controls

Proposed verification-layer amendment | for review and formal approval

This proposed implementation amendment accompanies the existing AML/CFT Policy v1.0. It does not record a new board approval or alter the original policy's approval history. The existing 16-page policy follows unchanged.

Sender identity verification

For SharpSharp onboarding and transfer readiness, the proposed Madiba Verify workflow links sender identity checks to the authenticated account. Country-supported national ID or passport checks, and approved alternatives such as BVN where available, supply evidence for the agreed decision policy.

Where required by the approved workflow, capture a live selfie, assess liveness and compare with an eligible identity image. Keep database validation, document authenticity, biometrics, sanctions screening and PEP review as separate evidence fields. Unresolved or suspicious results require review before clearance.

Recipient verification

Validate destination country, payout rail and bank/account or mobile money details. Resolve the account name through an authoritative provider where available; obtain required beneficiary information and screening under the relevant policy and partner allocation.

Clearly distinguish phone validity/carrier detection from account-name enquiry and ownership or identity verification. Do not label an unavailable check successful. Material mismatches or insufficient evidence block collection pending resolution.

Collection release condition

Collection may begin only after sender clearance, recipient checks, screening/review requirements, quote validity and executable payout readiness are all satisfied. Technical completion of a provider session does not constitute compliance approval or transfer authorization.

Evidence, review and rollout

Implementation requirements supporting existing policy sections 9, 12, 16, 18 and 19.

Account binding and controlled reuse

Store the provider reference, evidence categories, country, method, timestamps, decision, reviewer where applicable, policy version and expiry. Reuse sender clearance only within approved validity and risk rules. Trigger new checks when identity, beneficiary, risk or partner requirements change.

Integrity and access

Accept authoritative provider evidence through authenticated server-side integrations. Verify callback authenticity, handle duplicates and contradictory events, and record immutable decision history. Limit access to identity and biometric records; apply documented retention, deletion and authorized sharing rules.

Exceptions and accountability

Failed, suspicious, incomplete, expired and unavailable outcomes remain distinct. Define reviewer authority, escalation to the MLRO/Compliance Officer, partner notification and remediation. Alternative providers must meet the approved evidence policy; switching providers must not silently override a rejection.

Implementation and approval record

Before production release, document country/document coverage, accepted evidence, provider terms, consent/privacy wording, screening allocation, thresholds, manual review and retention. Confirm these with the relevant partners and responsible compliance reviewers.

Current rollout: live verification testing is review-only. Automatic sender approval and money transfers remain disabled. This amendment describes the intended layer and does not certify implementation or replace any applicable obligation.

Approval fields to complete separately: approving body / responsible owner / policy version / effective date / approved countries and rails / testing evidence / open conditions. No approval is implied by this document.

MADIBA DIGITALS, INC.
5614 Shagbark Place, Groveport, Ohio 43125, USA | info@madiba.digital | +1-614-377-0445

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

Including Counter-Proliferation Financing and Sanctions Controls

Document Owner	Akotarh Akoson — Money Laundering Reporting Officer / Compliance Officer
Policy Version	1.0
Effective Date	October 4, 2026
Review Cycle	At least annually and upon material regulatory, product, partner, or geographic change
Approved By	Board of Directors, MADIBA DIGITALS, INC.
Classification	Internal Corporate Policy / Controlled Document
Applies To	MADIBA DIGITALS, INC., MADIBA DIGITALS LTD, and relevant group personnel, contractors, products and operations

Policy Statement

MADIBA DIGITALS, INC. is committed to preventing its technology, products, partner integrations and business relationships from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption or other financial crime. The Company applies a risk-based compliance framework proportionate to its role as a technology and payment/remittance orchestration business and to the risks presented by its customers, counterparties, corridors, partners and products.

Approved Operating Model

Under the Company's approved operating model, MADIBA DIGITALS, INC. and MADIBA DIGITALS LTD provide technology, routing, integration and transaction-orchestration capabilities. Customer funds are intended to be collected and paid out by appropriately licensed or otherwise authorized third-party payment/remittance partners. Madiba shall not receive, hold, safeguard, store or settle customer funds in a Madiba-controlled customer funds account unless the Board first approves a changed operating model and applicable legal, licensing and compliance requirements are satisfied.

1. Purpose

This Anti-Money Laundering and Countering the Financing of Terrorism Policy establishes the minimum principles, governance arrangements, controls and escalation procedures by which MADIBA DIGITALS, INC. ("Madiba" or the "Company") seeks to identify, assess, mitigate, monitor and report risks relating to money laundering, terrorist financing, proliferation financing, sanctions evasion and related financial crime.

The Policy is intended to support responsible growth, partner onboarding, regulatory readiness and the integrity of Madiba's payment and remittance orchestration activities. It is designed to operate alongside applicable law, contractual obligations with regulated partners, product-specific procedures, cybersecurity controls, privacy requirements and internal risk management practices.

2. Scope

This Policy applies to MADIBA DIGITALS, INC.; MADIBA DIGITALS LTD, its Nigerian subsidiary; directors; officers; employees; contractors; consultants; relevant agents; and any person acting on behalf of a Madiba group company where their activities could expose the Company to financial-crime risk.

- all current and future Madiba payment, remittance, mobile-money, bank-transfer and orchestration products, including SharpSharp and Momo2Momo where applicable;
- all source and destination markets, transaction corridors, collection partners, payout partners, banks, mobile-money operators, payment service providers and other financial counterparties;
- customer-facing, partner-facing and internal technology that initiates, routes, authorizes, monitors, records or supports transactions;
- all business relationships for which Know Your Customer, Know Your Business, sanctions, beneficial ownership, source-of-funds or related due-diligence considerations may arise.

Where a local law, licence condition, partner agreement or regulator imposes a higher standard than this Policy, the higher standard shall apply. Where there is uncertainty, the matter must be escalated to the Money Laundering Reporting Officer / Compliance Officer before the activity proceeds.

3. Regulatory and Standards Framework

Madiba will maintain its compliance program with regard to applicable legal and regulatory requirements in each jurisdiction in which it operates or enables transactions. The following are particularly relevant to the Company's current structure and intended activities, to the extent applicable:

- United States Bank Secrecy Act and Financial Crimes Enforcement Network requirements, including rules applicable to Money Services Businesses and money transmission where the Company's actual facts and circumstances bring an activity within scope;
- United States economic and trade sanctions administered by the Department of the Treasury's Office of Foreign Assets Control;
- Financial Action Task Force Recommendations and risk-based guidance for money or value transfer services, digital payments, customer due diligence, beneficial ownership and targeted financial sanctions;
- Nigeria's Money Laundering (Prevention and Prohibition) Act, 2022; Terrorism (Prevention and Prohibition) Act, 2022; applicable Central Bank of Nigeria Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing regulations, guidelines and targeted financial sanctions requirements;
- requirements of the Nigerian Financial Intelligence Unit, Nigeria Sanctions Committee, Special Control Unit Against Money Laundering and other competent authorities where applicable;

- applicable laws and regulatory expectations in Ghana, Cameroon and any additional markets added to Madiba's network; and
- compliance requirements contractually imposed by Madiba's regulated collection, payout, banking and infrastructure partners.

Regulatory Classification

This Policy does not itself determine whether Madiba is or is not a regulated Money Services Business, money transmitter, payment service provider, international money transfer operator or equivalent regulated entity in any jurisdiction. Regulatory classification is a facts-and-circumstances determination and must be reviewed before launch of a new product, corridor, funds flow, custody model, partner arrangement or jurisdiction.

4. Business Model and Allocation of Responsibilities

Madiba's core proposition is technology-enabled orchestration. The Company connects appropriately vetted and authorized collection and payout partners through application programming interfaces, routing logic and transaction-management technology so that value can move from a sender to an intended recipient through regulated rails.

The operating model is designed around the following principles:

- The sender pays a licensed or otherwise authorized collection partner, not a Madiba customer-funds account.
- Madiba's systems may capture transaction instructions, recipient information, routing data, status information and compliance metadata necessary to orchestrate the transaction.
- The collection partner performs the regulated receipt/collection function and the payout partner performs the regulated disbursement function, subject to the allocation of duties in applicable agreements and law.
- Madiba may route transactions among eligible partners based on availability, jurisdiction, service capability, risk controls, price, settlement arrangements, speed and other approved factors.
- Madiba does not permit any routing logic to bypass a required sanctions, identity, transaction-monitoring, legal or partner control.
- Where one partner performs both collection and payout, Madiba may still provide orchestration, user experience, data exchange and status-management functions.

Partner reliance does not eliminate Madiba's responsibility to maintain controls appropriate to the risks arising from its own technology, data, commercial relationships and decisions. Madiba shall maintain sufficient visibility to identify unusual or prohibited activity and to cooperate with regulated partners and competent authorities.

5. Core Definitions

Term	Meaning
Anti-Money Laundering (AML)	Measures designed to prevent, detect and respond to efforts to disguise or legitimize proceeds derived from criminal activity.
Countering the Financing of Terrorism (CFT)	Measures designed to prevent, detect and disrupt the raising, movement or use of funds or other value for terrorist acts, terrorists or terrorist organizations.
Counter-Proliferation Financing (CPF)	Measures designed to prevent, detect and disrupt

	financing connected to the proliferation of weapons of mass destruction, including compliance with targeted financial sanctions.
Customer Due Diligence (CDD)	The process of identifying and verifying customers, understanding the purpose and intended nature of the relationship, assessing risk and conducting ongoing monitoring.
Enhanced Due Diligence (EDD)	Additional due diligence applied where risk is higher, such as higher-risk jurisdictions, unusual activity, complex ownership, adverse information or politically exposed persons.
Know Your Customer (KYC)	Identity verification and related checks performed on individual customers.
Know Your Business (KYB)	Verification and risk assessment of legal entities, including incorporation, ownership, controllers, business purpose, licensing and sanctions screening.
Money Laundering Reporting Officer (MLRO)	The senior person designated to oversee the Company's AML/CFT program, receive internal suspicious-activity escalations and coordinate any reporting or cooperation obligations.
Politically Exposed Person (PEP)	A person entrusted with a prominent public function, and where required by applicable law or policy, relevant family members and close associates.
Ultimate Beneficial Owner (UBO)	The natural person who ultimately owns or controls a legal entity or on whose behalf a transaction or activity is conducted.
Suspicious Activity / Suspicious Transaction	Activity for which there are reasonable grounds to suspect a connection to money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud or other criminal conduct.
Targeted Financial Sanctions (TFS)	Asset-freezing and related prohibitions imposed against designated persons, entities, vessels, groups, countries or activities under applicable sanctions regimes.

6. Governance and Accountability

6.1 Board of Directors

The Board of Directors has ultimate oversight of this Policy and the effectiveness of the Company's AML/CFT framework. The Board shall:

- approve this Policy and material amendments;
- designate a competent Money Laundering Reporting Officer / Compliance Officer with sufficient authority, access and independence, and formally record the appointment;
- ensure adequate financial, technical and human resources are available for compliance;
- receive periodic reporting on material financial-crime risks, significant partner issues, suspicious-activity trends, sanctions alerts, compliance incidents and remediation;

- approve material changes to the operating model that could change Madiba's regulatory classification or custody of customer funds.

6.2 Money Laundering Reporting Officer / Compliance Officer

Akotarh Akoson is designated by the Board of Directors as the Money Laundering Reporting Officer (MLRO) and Compliance Officer of MADIBA DIGITALS, INC., effective October 4, 2026. He serves concurrently as Board Chairman and Executive Director. In his compliance capacity, he is the designated owner of this Policy and has direct access to the Board, senior management, relevant personnel, systems, records and partner information reasonably necessary to discharge the role. The responsibilities of the MLRO / Compliance Officer include:

- maintaining the enterprise financial-crime risk assessment and risk-based procedures;
- reviewing high-risk customers, partners, corridors and escalated transactions;
- receiving and documenting internal suspicious-activity reports;
- determining whether external reporting or partner escalation is required;
- maintaining sanctions, politically exposed person and adverse-media escalation processes;
- coordinating training, monitoring, testing and remediation;
- maintaining records sufficient to evidence compliance;
- reporting directly to senior management and the Board on material matters.

Independence and conflict management. The MLRO / Compliance Officer may escalate any material anti-money laundering, countering the financing of terrorism, sanctions, fraud or related compliance matter directly to the Board without prior management approval. Where a matter concerns the conduct, personal interests or potential conflict of the MLRO / Compliance Officer, the matter shall be referred directly to the other directors who are not involved in the matter for independent review and decision, and the MLRO / Compliance Officer shall not control, suppress or determine the disposition of that matter.

6.3 Chief Executive Officer

The Chief Executive Officer is responsible for ensuring that business execution, customer operations, partner onboarding and commercial activity operate within approved compliance parameters and that compliance requirements are incorporated into operational plans.

6.4 Chief Technology Officer

The Chief Technology Officer is responsible for embedding required controls into the technology environment, including secure application programming interface integrations, identity and authorization logic, immutable or tamper-evident logging where appropriate, access controls, transaction rules, sanctions/monitoring integrations, incident response support and the ability to suspend or block transactions when required.

6.5 Board Operations, Support and Partnerships Coordinator

The Board Operations, Support and Partnerships Coordinator supports the governance and partner-management process by tracking partner onboarding status, outstanding Know Your Business requests, due dates, documentation requests, meeting follow-ups and unresolved partner responses. This role does not make compliance approvals or override the Money Laundering Reporting Officer, but must promptly escalate compliance-sensitive matters to the appropriate officer or director.

6.6 All Personnel

Every director, officer, employee and contractor is responsible for complying with this Policy, completing required training, protecting confidential information, reporting concerns promptly and refraining from tipping off a customer or third party about a suspicious-activity review or report where prohibited.

7. Financial Crime Risk Appetite and Prohibited Activity

Madiba has no appetite for knowingly facilitating money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption or other criminal activity. The following are prohibited unless expressly permitted by applicable law, approved by the Board after documented legal/compliance review, and supported by appropriate controls:

- anonymous or fictitious customers;
- transactions involving persons or entities subject to applicable asset-freezing or blocking sanctions;
- transactions where the sender, recipient, source of funds, destination or purpose cannot be reasonably established when required;
- use of Madiba products to obscure beneficial ownership, evade reporting thresholds, bypass partner controls or conceal transaction origin/destination;
- cash collection by Madiba personnel or into Madiba-controlled accounts;
- holding customer balances or stored value by Madiba;
- cryptocurrency or virtual-asset collection/payout unless separately approved following legal classification and risk assessment;
- transactions connected to prohibited goods, illegal services, human trafficking, terrorism, sanctions evasion or other unlawful activity;
- relationships with unlicensed or unauthorized partners where a licence or authorization is required for the role performed.

8. Enterprise and Product Risk Assessment

Madiba shall apply a documented risk-based approach. Risk assessments shall consider inherent risk, strength of controls and residual risk. At a minimum, the following risk dimensions shall be considered before launch and periodically thereafter:

- **Customer risk:** customer type, identity reliability, occupation/business, ownership complexity, transaction history, politically exposed person status, adverse information and expected activity;
- **Geographic risk:** source and destination countries, sanctions exposure, corruption and financial-crime risk, regulatory maturity, conflict/instability, Financial Action Task Force public statements and partner restrictions;
- **Product and service risk:** cross-border remittance, mobile-money payout, bank payout, speed, irreversibility, transaction limits, ability to transact remotely and fraud exposure;
- **Delivery-channel risk:** non-face-to-face onboarding, device/network indicators, application programming interfaces, third-party identity tools and digital-only customer interaction;
- **Transaction risk:** value, frequency, velocity, pattern, sender-recipient relationship, funding method, payout method, retries, reversals and chargebacks;
- **Partner risk:** licensing status, compliance maturity, ownership, sanctions exposure, financial condition, service countries, data quality, audit history and control effectiveness;
- **Technology risk:** system vulnerabilities, access controls, data integrity, model/rules quality, alert failures, integration defects and cyber-enabled fraud.

A material change in product design, funds flow, jurisdiction, customer segment, transaction limit, partner, ownership, regulatory status or technology shall trigger a targeted risk review before implementation where practicable.

9. Customer Identification, Verification and Due Diligence

Because Madiba's collection and payout partners perform regulated financial functions, customer identification and verification may be performed directly by the regulated partner, by Madiba using approved tools, or through a coordinated process. The allocation must be documented in the relevant partner agreement and technical integration.

No transaction may proceed unless the minimum identity and compliance conditions required by applicable law, the relevant regulated partner and Madiba's risk controls have been satisfied.

9.1 Individual Customers

- Collect or receive sufficient identity information to uniquely associate a transaction with the sender, subject to the applicable partner model and law.
- Use reliable, independent data, documents or approved digital identity methods where direct verification is required.
- Capture or receive confirmation of sanctions and politically exposed person screening where required.
- Understand expected transaction purpose, corridor and activity where the risk profile or partner rules require it.
- Apply Enhanced Due Diligence when risk is elevated.

9.2 Recipients / Beneficiaries

- Capture the recipient information required for the selected payout method, such as name, mobile number, wallet identifier or bank details.
- Where available, use name-enquiry, wallet-verification or partner confirmation capabilities to reduce misdirected payments and identity risk.
- Screen recipients against applicable sanctions lists when required by law, partner controls or Madiba's risk rules.

9.3 Reliance on Partner KYC

Where Madiba relies on a regulated partner's Know Your Customer process, Madiba shall obtain reasonable assurance that the partner maintains an appropriate customer due diligence program, performs required screening, retains records and can provide relevant information where lawfully requested. Reliance shall not be used to deliberately avoid a legal obligation that applies directly to Madiba.

10. Know Your Business and Counterparty Due Diligence

Before onboarding a collection partner, payout partner, payment service provider, bank, mobile-money operator, major technology provider or other material financial counterparty, Madiba shall perform risk-based Know Your Business due diligence. The review should include, as applicable:

- legal name, registration number, jurisdiction of incorporation and registered/principal business address;
- directors, controllers and Ultimate Beneficial Owners;
- regulatory licences, registrations or authorizations relevant to the services being provided;
- sanctions, politically exposed person and adverse-media screening of the entity and relevant owners/controllers;
- Anti-Money Laundering and Countering the Financing of Terrorism framework, customer due diligence controls, transaction monitoring, suspicious-activity reporting, targeted financial sanctions processes and compliance governance;
- service scope, countries, collection/payout methods, settlement model and use of subcontractors or downstream partners;

- information-security and privacy posture where the partner handles sensitive data;
- contractual rights to suspend transactions, request information, investigate alerts, terminate for compliance reasons and cooperate on regulatory inquiries.

High-risk or strategically critical partners may require Enhanced Due Diligence, legal review, references, independent licence verification, compliance attestations, audit reports or direct compliance discussions before activation.

11. Beneficial Ownership, Politically Exposed Persons and High-Risk Relationships

Where the Company onboards a legal entity or relies on a legal entity in a material transaction flow, reasonable steps shall be taken to identify and verify the natural persons who ultimately own or control that entity, consistent with applicable thresholds and partner/regulatory requirements.

A Politically Exposed Person is not automatically prohibited. However, relationships involving a Politically Exposed Person require risk-based Enhanced Due Diligence, appropriate senior approval, reasonable source-of-wealth/source-of-funds consideration where relevant, and enhanced ongoing monitoring. Family members and close associates shall be handled as required by applicable law and risk.

12. Sanctions and Targeted Financial Sanctions

Madiba shall maintain a risk-based sanctions compliance process consistent with its U.S. nexus, operating jurisdictions and partner obligations. Screening sources shall include, as applicable, the United States Office of Foreign Assets Control sanctions lists, United Nations Security Council sanctions, Nigeria Sanctions Committee designations and other lists required by applicable law or partner contracts.

- Screen relevant customers, recipients, partners, directors, beneficial owners and transaction parties at onboarding and, where required, on an ongoing or transactional basis.
- Use appropriate name-matching logic and review potential matches before release of a transaction where required.
- Immediately suspend, reject or block activity when required by applicable sanctions law, partner instruction or competent authority, and escalate to the Money Laundering Reporting Officer / Compliance Officer.
- Do not inform a customer how to circumvent a sanctions control or modify transaction data to avoid a match.
- Document sanctions decisions, including false-positive clearance rationale and true-match escalation.

Sanctions controls shall be tested periodically and after material changes to screening systems, lists, thresholds, integrations or routing logic.

13. Transaction Monitoring and Financial-Crime Detection

Madiba shall maintain monitoring proportionate to the data and control points available to it. Monitoring may combine automated rules, partner-generated alerts, device/network intelligence, fraud indicators, sanctions results and manual review.

Examples of potentially suspicious or higher-risk patterns include:

- rapid or repeated transactions inconsistent with expected customer behavior;
- multiple senders using common devices, payment instruments or identifiers to send to one recipient without a reasonable explanation;
- one sender distributing value to many unrelated recipients in a short period;
- attempts to structure transactions just below partner or regulatory thresholds;
- repeated failed identity, sanctions or payment attempts followed by altered customer data;

- unusual transaction velocity, reversals, chargebacks, refunds or account changes;
- sender and recipient information that appears fabricated, inconsistent or linked to known fraud/mule indicators;
- activity involving high-risk jurisdictions or corridors inconsistent with the stated purpose;
- unexplained third-party funding or payment instruments not reasonably linked to the sender;
- evidence of trafficking, scams, business-email compromise, account takeover, terrorist financing or sanctions evasion;
- unusual routing behavior, manual overrides or attempts to bypass controls.

No individual red flag necessarily proves unlawful conduct. Alerts must be assessed in context, documented and escalated where suspicion remains.

14. Internal Suspicious-Activity Escalation and External Reporting

Any director, employee or contractor who knows, suspects or has reasonable grounds to suspect that activity may involve money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud or other serious financial crime must escalate the matter promptly to the Money Laundering Reporting Officer / Compliance Officer using the approved internal channel.

The Money Laundering Reporting Officer / Compliance Officer shall document the review, determine whether additional information is required, decide whether the transaction or relationship should be restricted, and determine whether an external report or partner escalation is legally or contractually required.

Where a reporting duty applies directly to Madiba, the Money Laundering Reporting Officer / Compliance Officer shall ensure that the relevant Suspicious Activity Report, Suspicious Transaction Report or equivalent filing is made to the appropriate authority within the applicable timeframe. Where the legal reporting duty sits with a licensed collection or payout partner, Madiba shall provide relevant information and cooperate with the partner's investigation and reporting process, subject to law and data-protection requirements.

Personnel must not disclose to the subject of a review that a suspicious-activity report has been or may be filed, or disclose information that could prejudice an investigation, where such disclosure is prohibited by law.

15. Source of Funds and Source of Wealth

Source-of-funds information concerns the origin of money used in a specific transaction or relationship. Source-of-wealth information concerns how a customer or beneficial owner accumulated overall wealth. Madiba or its regulated partners may request such information when required by law, partner rules or the risk profile.

- Enhanced inquiries may be appropriate for unusually large transfers, unexplained high velocity, high-risk customers, politically exposed persons, complex corporate structures or activity inconsistent with known profile.
- Acceptable evidence depends on context and may include employment income, business income, sale proceeds, investment statements, inheritance evidence or other reliable documentation.
- Transactions shall not proceed where required source-of-funds evidence is materially deficient and the risk cannot be satisfactorily mitigated.

16. Transaction Limits, Controls and Routing Governance

Transaction and velocity limits shall be established based on product design, partner rules, jurisdiction, customer risk, fraud experience and regulatory requirements. Limits may differ by corridor, customer tier, payout method or partner.

Routing logic may optimize across approved partners, but compliance controls are mandatory constraints. A transaction shall not be routed to a different partner for the purpose of avoiding sanctions, customer due diligence, suspicious-activity monitoring, reporting thresholds or legal restrictions.

Manual overrides of compliance-related blocks must be restricted, logged and subject to authorization by appropriately designated personnel. Material override activity shall be reviewable by Compliance and Technology leadership.

17. Ongoing Partner Oversight

Partner due diligence is not a one-time exercise. Madiba shall maintain a current partner register and periodically reassess material partners based on risk. Ongoing oversight should include:

- licence or registration status and material regulatory developments;
- service availability, countries, products and downstream dependencies;
- Know Your Business refreshes and beneficial-ownership changes;
- material compliance incidents, enforcement actions or adverse information;
- quality and timeliness of sanctions, customer due diligence, transaction-status and investigation data;
- contractual service levels, dispute rates, chargebacks, suspicious patterns and fraud losses;
- periodic compliance attestations, questionnaires or meetings where appropriate.

A partner may be suspended, restricted or terminated where Madiba is not satisfied that identified financial-crime risks are being adequately controlled.

18. Recordkeeping and Audit Trail

Madiba shall maintain complete, accurate and retrievable records sufficient to reconstruct material compliance decisions and transaction events. Unless a longer period is required, relevant AML/CFT records should be retained for at least five years after the transaction, relationship termination or decision to which the record relates.

- customer and partner due-diligence records and verification results;
- beneficial-ownership, politically exposed person, sanctions and adverse-media screening results;
- transaction instructions, routing decisions, timestamps, identifiers and status events available to Madiba;
- alerts, investigations, internal reports, escalation decisions and supporting rationale;
- partner compliance correspondence and onboarding evidence;
- training, testing, risk assessments, Board reporting and policy approvals.

Records shall be protected against unauthorized access, alteration or destruction and shall be made available to competent authorities or regulated partners when lawfully required.

19. Data Protection, Confidentiality and Information Sharing

AML/CFT controls frequently require sensitive identity, transaction and investigation data. Madiba shall limit collection and sharing to information reasonably necessary for legitimate business, compliance, legal and security purposes and shall apply appropriate access controls, encryption, retention controls and confidentiality protections.

Information may be shared with collection partners, payout partners, banks, identity-verification providers, sanctions-screening vendors, law enforcement or regulators where authorized or required by law, contract or the transaction model. Suspicious-activity reporting information shall receive heightened confidentiality protection.

20. Personnel Screening and Training

Madiba shall apply proportionate pre-employment or pre-engagement screening for personnel in sensitive roles, subject to applicable law. Screening may include identity verification, employment history, references, conflicts of interest and criminal or regulatory checks where lawful and appropriate.

AML/CFT training shall be provided at onboarding and at least annually thereafter for relevant personnel. Role-specific training shall be provided to directors, executives, engineers, operations staff, partner-management personnel and the Money Laundering Reporting Officer / Compliance Officer as appropriate.

- money laundering, terrorist financing and proliferation financing concepts;
- Madiba's orchestration model and allocation of responsibilities with regulated partners;
- Know Your Customer, Know Your Business and beneficial-ownership controls;
- sanctions and politically exposed person requirements;
- transaction red flags, suspicious-activity escalation and anti-tipping-off rules;
- fraud, cyber-enabled financial crime and account-takeover indicators;
- recordkeeping, confidentiality and escalation responsibilities.

21. Monitoring, Testing and Independent Review

The effectiveness of the AML/CFT framework shall be evaluated through periodic control monitoring and independent review proportionate to the Company's size, complexity and risk. Once transaction services are live, an independent assessment should occur at least annually, or more frequently where risk, law, partner requirements or material changes justify it.

Testing should evaluate governance, customer and partner due diligence, sanctions screening, transaction monitoring, alert handling, suspicious-activity escalation, recordkeeping, training, technology controls and remediation. Material findings shall be assigned owners, target dates and Board visibility where appropriate.

22. Compliance Incidents, Breaches and Remediation

Potential breaches of this Policy, sanctions controls, customer due diligence requirements, partner obligations or financial-crime controls must be reported promptly to the Money Laundering Reporting Officer / Compliance Officer and the responsible executive.

Material incidents shall be documented with root cause, affected transactions/partners, containment, legal/regulatory analysis, notification obligations, corrective actions, owner and due date. Technology defects affecting financial-crime controls shall receive priority consistent with their risk and may require transaction suspension until controls are restored.

23. New Products, Markets, Corridors and Material Changes

Before launching a new country, corridor, payment method, collection arrangement, payout arrangement, funding method, partner, product or material technology change, the responsible business and technology owners shall complete a compliance impact review. The review must consider regulatory classification, licensing dependencies, sanctions exposure, customer due diligence, transaction monitoring, data requirements, partner responsibilities, transaction limits and reporting obligations.

No product change may introduce direct custody, safeguarding or settlement of customer funds by Madiba without specific Board approval and documented legal/compliance analysis.

24. Violations and Disciplinary Consequences

Violation of this Policy may result in restriction of access, reassignment of duties, disciplinary action, termination of employment or contract, suspension of a partner relationship, escalation to the Board and, where required, reporting to competent authorities. No person shall suffer retaliation for raising a good-faith compliance concern.

25. Policy Review and Approval

This Policy shall be reviewed at least annually and sooner where there is a material change in law, regulatory expectations, ownership, business model, products, jurisdictions, partners, transaction flows or risk profile. Amendments shall be approved in accordance with the Company's governance framework.

Appendix A — Minimum AML/CFT Control Framework

Control Area	Minimum Standard
Governance	Board approval; designated Money Laundering Reporting Officer / Compliance Officer; periodic reporting; documented responsibilities.
Risk Assessment	Enterprise and product/corridor risk assessment; periodic refresh; documented residual risk.
Customer Due Diligence	Identity verification directly or through regulated partners; risk rating; ongoing monitoring; Enhanced Due Diligence where appropriate.
Know Your Business	Legal entity verification, licensing, beneficial ownership, sanctions, compliance-program review and ongoing partner refresh.
Sanctions	Applicable sanctions screening; alert review; transaction hold/block/reject capability; records and testing.
Transaction Monitoring	Risk-based rules, partner alerts, device/fraud indicators, investigation and documented disposition.
Suspicious Activity	Internal escalation; Money Laundering Reporting Officer review; external reporting or partner cooperation where required; confidentiality.
Recordkeeping	At least five years unless longer required; retrievable audit trail; secure storage.
Training	Onboarding and annual training; role-specific content.
Independent Review	At least annual once live, or more frequently as risk/requirements dictate; remediation tracking.
Technology Controls	Access control, logging, integrity, alerting, change management, override controls and blocking capability.
Partner Oversight	Partner register, periodic review, compliance attestations, incident escalation and termination rights.

Appendix B — Illustrative Risk Rating Method

The following approach may be used for customer, partner, corridor or product risk assessments. It is illustrative and may be refined by Compliance as data and regulatory requirements develop.

Factor	Lower Risk Indicators	Higher Risk Indicators	Example

			Weight
Geography	Established, well-regulated market; low sanctions exposure	Sanctions concerns; weak controls; conflict/high corruption; FATF public statement	20%
Customer	Verified identity; transparent profile; expected activity	PEP; identity anomalies; adverse information; unexplained activity	20%
Transaction	Low/normal value and velocity; clear purpose	High velocity; structuring; unusual value; reversals; third-party funding	25%
Partner	Licensed; mature AML/CFT controls; good data	Unclear licensing; weak controls; enforcement/adverse media	20%
Product/Channel	Controlled limits; strong authentication	High speed/irreversibility; anonymous features; weak authentication	15%

Risk categories should normally be Low, Medium or High. A High rating requires documented Enhanced Due Diligence, senior/compliance approval where applicable and enhanced monitoring. Prohibited activity must not be approved merely because Enhanced Due Diligence was performed.

Appendix C — Transaction and Behavioral Red Flags

- Sender repeatedly changes recipient details after failed compliance or payment checks.
- Multiple accounts, phone numbers or devices appear controlled by one person without a reasonable explanation.
- One recipient receives funds from numerous unrelated senders in a short period.
- Customer repeatedly transacts just below limits or thresholds.
- Customer refuses or evades reasonable identity, purpose, source-of-funds or beneficial-ownership questions.
- Transaction purpose is inconsistent with customer profile, geography or relationship to recipient.
- Unusual chargebacks, refunds, payment reversals, disputed card usage or rapid retry behavior.
- Use of compromised accounts, mule indicators, synthetic identity patterns or scam typologies.
- Connection to high-risk jurisdictions, sanctioned parties, terrorism indicators or prohibited goods/services.
- Partner data is materially inconsistent across identity, payment and payout records.
- Employee or contractor attempts to bypass or suppress a compliance alert without appropriate authority.
- Repeated manual routing to a partner with weaker controls or limits without a legitimate operational reason.

Appendix D — Partner AML/KYB Due Diligence Checklist

- ☐ Certificate of incorporation / company registry extract
- ☐ Business address and principal contacts
- ☐ Ownership and Ultimate Beneficial Owner information
- ☐ Directors and key controllers
- ☐ Relevant licences / regulatory registrations / authorizations

- ☐ AML/CFT/CPF policy or compliance attestation
- ☐ Name and role of Money Laundering Reporting Officer / Compliance Officer
- ☐ Customer Due Diligence / Know Your Customer framework
- ☐ Sanctions and Politically Exposed Person screening framework
- ☐ Transaction monitoring and suspicious-activity reporting process
- ☐ Countries and payment methods supported
- ☐ Collection, settlement and payout funds-flow description
- ☐ Downstream providers / subcontractors relevant to the service
- ☐ Information-security / data-protection review as applicable
- ☐ Adverse media / enforcement / sanctions screening
- ☐ Contractual compliance, audit, suspension and termination rights
- ☐ Periodic refresh date and risk rating

Appendix E — Internal Escalation Path

Event	Immediate Action	Primary Owner	Escalation
Potential sanctions match	Pause/hold as technically and legally appropriate; do not override	Compliance / Operations	MLRO; CTO if system action needed; Board for material case
Suspicious transaction pattern	Preserve data; do not alert customer to suspicion	Operations / Compliance	MLRO; regulated partner as required
Partner compliance concern	Pause new onboarding or affected route if risk warrants	Partnerships / Compliance	CEO, CTO, MLRO; Board if material
AML control system failure	Contain defect; assess affected transactions; prioritize remediation	CTO / Engineering	MLRO, CEO; Board for material impact
Regulatory inquiry	Preserve records; route centrally; avoid unauthorized response	MLRO / Authorized Officer	Board and legal counsel as appropriate
Employee bypass / misconduct	Restrict access if necessary; preserve evidence	Management / Compliance	Board; HR/legal as appropriate

Appendix F — Reference Framework

This Policy has been drafted with regard to the following regulatory and international frameworks, as amended from time to time and to the extent applicable to Madiba's activities:

- Financial Action Task Force (FATF) Recommendations and risk-based guidance, including guidance for Money or Value Transfer Services.
- United States Bank Secrecy Act and Financial Crimes Enforcement Network regulations and guidance concerning Money Services Businesses and money transmission.
- United States Department of the Treasury, Office of Foreign Assets Control — A Framework for OFAC Compliance Commitments.
- Nigeria Money Laundering (Prevention and Prohibition) Act, 2022.

- Nigeria Terrorism (Prevention and Prohibition) Act, 2022.
- Central Bank of Nigeria Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing framework, regulations, licensing guidance and targeted financial sanctions guidance.
- Applicable local AML/CFT, sanctions, payment-services, privacy and financial-crime requirements in each market in which Madiba or its partners operate.

Nothing in this Policy should be interpreted as a legal opinion that Madiba is exempt from any licence, registration, reporting or regulatory requirement. The Company shall obtain jurisdiction-specific legal or regulatory advice where the classification or obligations of a product, corridor or funds flow are uncertain.

Policy Approval Record

This Policy is adopted as a corporate compliance policy of MADIBA DIGITALS, INC. and shall become effective on the date approved by the Board of Directors. The Board may approve the Policy by signature below, written consent or formal Board resolution in accordance with the Company's governance documents.

Name	Capacity	Signature / Date
Akotarh Akoson	Board Chairman & Executive Director	Oct 4, 2026
Divine Achu Akere	Founder, Vice Board Chairman & Chief Technology Officer	
Eyram Dela Kuwornu	Chief Executive Officer & Director	

MLRO / Compliance Officer Designation

Board designation. The Board of Directors has designated Akotarh Akoson to serve as the Company's Money Laundering Reporting Officer (MLRO) and Compliance Officer pursuant to a Board resolution effective October 1, 2026.

Name	Akotarh Akoson
Title	Money Laundering Reporting Officer (MLRO) & Compliance Officer
Effective Date	October 4, 2026
Signature	Oct 4, 2026