Anti-Money Laundering (AML) Policy Document

Organisation: AfriTech Bridge
Platforms: afritechbridge.online | study.afritechbridge.online | jobs.afritechbridge.online
Registered Office: Kigali, Rwanda
Policy Reference: ATB-AML-001
Version: 1.0
Effective Date: 21 February 2026
Next Review Date: 21 February 2027
Document Owner: Compliance Officer, AfriTech Bridge

Table of Contents

1. Introduction & Purpose

AfriTech Bridge ("AfriTech Bridge", "the Company", "we") is a technology-enabled organisation headquartered in Kigali, Rwanda, operating three interconnected digital platforms:

Platform	Domain	Function
AfriTech Bridge	afritechbridge.online	Corporate identity, partnerships, programme information
AfriTech Bridge LMS	study.afritechbridge.online	Online learning management system — practical tech training for African youth including rural and underserved communities
AfriTech Opportunities	jobs.afritechbridge.online	Job listings, scholarship discovery, career resources, employer recruitment solutions

The Company's operations involve the collection and processing of fees from learners, employers, scholarship sponsors, and partner organisations. These financial flows — however small individually — expose the Company to the risk of being used, knowingly or unknowingly, as a conduit for money laundering (ML) or terrorist financing (TF).

1.1 Purpose

This Anti-Money Laundering Policy ("the Policy") establishes the framework by which AfriTech Bridge:

- Prevents, detects, and reports money laundering and terrorist financing activity.
- Meets its obligations under applicable Rwandan law, East African Community (EAC) directives, and international best practices.
- Protects the integrity, reputation, and financial safety of all platforms.
- Provides clear guidance to every employee, contractor, partner, and agent acting on behalf of the Company.

1.2 Policy Statement

AfriTech Bridge has zero tolerance for money laundering, terrorist financing, bribery, corruption, and any other financial crime. The Company is committed to implementing proportionate, risk-based controls across all platforms and business functions. Compliance with this Policy is mandatory for all personnel.

---

2. Scope of Application

This Policy applies to:

- **All employees** (full-time, part-time, remote) of AfriTech Bridge.
- **Contractors, consultants, freelancers, and agents** acting on behalf of the Company.
- **All business units and platforms**: LMS, Job Portal, and corporate website.
- **All financial transactions** processed through or associated with AfriTech Bridge services, including but not limited to:
- Course application fees and programme tuition payments.
- Employer job-posting fees, featured-ad payments, and recruitment solution subscriptions.
- Scholarship disbursements and sponsor contributions.
- Partner and vendor payments.

- Donation or grant receipts.
- Any future financial products introduced by the Company.

3. Legal & Regulatory Framework

AfriTech Bridge operates primarily in Rwanda and serves users across the African continent. The following laws, regulations, and standards govern this Policy:

3.1 Rwanda

Reference	Description
Law No. 74/2013 of 11/09/2013	Law on prevention and penalisation of money laundering and financing of terrorism
Law No. 47/2008 of 09/09/2008	Penal Code provisions on financial crime
National Bank of Rwanda (BNR) Directives	Applicable AML/CFT directives for financial service providers and non-financial businesses
Rwanda Investigation Bureau (RIB)	Financial Investigation Unit (FIU-Rwanda) reporting obligations
Rwanda Development Board (RDB)	Business registration and Good Governance compliance

3.2 International Standards

Reference	Description
FATF 40 Recommendations	Financial Action Task Force international AML/CFT standards
FATF Guidance on Digital ID	Customer due diligence using digital identity verification
Egmont Group Principles	Financial Intelligence Unit cooperation
UN Security Council Resolutions	Sanctions and asset freeze obligations
EAC AML Framework	East African Community regional AML harmonisation

3.3 Cross-Border Obligations

Where AfriTech Bridge processes payments from or to users outside Rwanda, the Company will apply the higher standard between Rwandan law and the law of the counterparty's jurisdiction.

4. Definitions

Term	Definition
Money Laundering (ML)	The process of making illegally obtained funds appear legitimate, typically through placement, layering, and integration.
Terrorist Financing (TF)	Providing or collecting funds, by any means, with the intention or knowledge that they will be used to carry out terrorist acts.
Customer Due Diligence (CDD)	The process of verifying and understanding the identity and intentions of customers.
Know Your Customer (KYC)	Procedures to verify the identity of individual users/learners before or during onboarding.
Know Your Business (KYB)	Procedures to verify corporate entities — employers, sponsors, or partners — before entering commercial relationships.
Enhanced Due Diligence (EDD)	A higher level of scrutiny applied to high-risk customers, transactions, or jurisdictions.
Simplified Due Diligence (SDD)	Reduced verification procedures for demonstrably low-risk customers or transactions.
Suspicious Transaction Report (STR)	A formal report submitted to the Financial Intelligence Unit (FIU) upon identification of suspicious activity.
Politically Exposed Person (PEP)	An individual who is or has been entrusted with a prominent public function, and their immediate family members and close associates.
Beneficial Owner	The natural person(s) who ultimately own or control a corporate entity or on whose behalf a transaction is conducted.
Shell Company	A company with no genuine business activity, often used to obscure the ownership of funds.
Smurfing	The practice of structuring large amounts of money into smaller transactions to evade detection thresholds.
FIU	Financial Intelligence Unit — Rwanda's competent authority for receiving STRs.
Compliance Officer	The designated senior individual responsible for AML oversight at AfriTech Bridge.

5. AML Risk Assessment

5.1 Business-Wide Risk Profile

AfriTech Bridge operates in a sector — EdTech, job marketplace, and digital services — that carries **low-to-medium** inherent ML/TF risk compared to financial services. However, specific risk factors must be managed actively.

5.2 Risk Factors by Platform

5.2.1 LMS — study.afritechbridge.online

Risk Factor	Risk Level	Rationale
Low-value individual transactions	Low	Most learners pay modest course fees; volume remains limited
Free/sponsored training programmes	Low	No direct learner payments; sponsor onboarding required
Anonymous or unverified applications	Medium	AI-fair selection process requires adequate identity checks prior to payment collection
Payments from high-risk jurisdictions	Medium	Pan-African user base may include FATF-listed jurisdictions
Scholarship fund disbursements	Medium	Outgoing transfers could be misused if sponsor intent is unclear

5.2.2 Job Portal — jobs.afritechbridge.online

Risk Factor	Risk Level	Rationale
Employer job-posting fees	Low-Medium	Businesses paying for listings — KYB required for corporate clients
Featured ads and premium subscriptions	Medium	Recurring and potentially high-value; source-of-funds verification needed
Candidate identity verification	Low	Free registration; no funds flow from job seekers
Salary guide and resume-builder tools	Negligible	Informational tools; no financial exposure
International employers	Medium	Cross-border entity verification needed for non-Rwandan business clients

5.2.3 Corporate Platform — afritechbridge.online

Risk Factor	Risk Level	Rationale
Partnership and grant agreements	Medium	Sponsorship or grant receipts from unknown organisations require due diligence
Vendor and supplier payments	Low	Standard procurement due diligence applies

5.3 Overall Residual Risk Rating: LOW-MEDIUM

This risk rating will be reviewed annually or upon any material change to the Company's business model, product offering, or regulatory environment.

6. Customer Due Diligence (CDD) & Know Your Customer (KYC)

6.1 Principles

AfriTech Bridge applies a **risk-based approach** to CDD. The level of due diligence is proportionate to the risk presented by the customer, transaction type, and geographic location.

6.2 When CDD is Required

CDD must be performed:

- Before accepting any payment or financial commitment from a learner or user.
- Before establishing an ongoing commercial relationship with any employer, sponsor, or partner.
- When a transaction or series of transactions is unusual, large, or inconsistent with known customer behaviour.
- Whenever there are grounds for suspecting ML/TF, regardless of transaction size.
- When there are doubts about the accuracy of previously collected identity information.

6.3 Standard CDD — Individual Learners & Users

For learners registering on the LMS or job seekers on the portal, the following information must be collected and verified:

Identity Verification (at minimum):
- Full legal name (as per national identification document).
- Date of birth.
- Nationality and country of residence.
- Residential address.
- Valid government-issued photo ID (National ID card, Passport, or Driver's licence).
- Contact details: active phone number and email address.

Verification Method:
- Document upload with automated or manual review.
- Cross-reference against the registration details supplied.
- Liveness or selfie check for high-value enrolment fees or where risk indicators exist.

6.4 Simplified Due Diligence (SDD)

SDD may be applied where:

- The learner is accessing a **free or fully-sponsored programme** with no financial transaction.
- The transaction value is below RWF 50,000 (approximately USD 40) and no risk flags are present.
- The customer has been verified previously and no new risk factors have emerged.

Even under SDD, basic registration data (name, email, phone, country) must still be collected.

6.5 Enhanced Due Diligence (EDD)

EDD must be applied when:

- The customer is identified as a PEP or close associate of a PEP.
- The customer is resident in or the payment originates from a FATF high-risk or non-cooperative jurisdiction.
- The transaction value is unusually high relative to the platform's typical transaction profile.
- The customer has previously triggered a suspicious activity flag.
- The payment method is obscure, unconventional, or difficult to trace (e.g. cryptocurrency, third-party wire transfers).

EDD Measures include:
- Verification of source of funds and source of wealth.
- Additional identity documentation.
- Senior management approval before onboarding.
- Ongoing enhanced monitoring of the account.

6.6 Ongoing Monitoring

CDD is not a one-time exercise. The Company will:

- Monitor customer activity throughout the relationship.
- Re-verify identity when information becomes outdated or inaccurate.
- Re-screen customers against sanctions and PEP lists periodically.
- Close or freeze accounts where CDD cannot be satisfactorily completed.

7. Know Your Business (KYB) – Employer & Partner Onboarding

7.1 Scope

All corporate entities — including employers posting jobs, scholarship sponsors, training partners, and corporate donors — are subject to KYB before a commercial relationship is established.

7.2 KYB Requirements

Documentation to be collected:

- Certificate of Incorporation or business registration certificate.
- Memorandum and Articles of Association (or equivalent constitutional document).
- List of directors and senior management.
- Beneficial ownership declaration (identifying any natural person owning ≥ 25% of the entity).
- Proof of registered business address.
- Tax Identification Number (TIN) or equivalent.
- Details of the authorised representative and their personal identity documents.

Verification:
- Companies based in Rwanda: verify against the Rwanda Development Board (RDB) company registry.
- Foreign companies: verify against the relevant national business registry of the jurisdiction of incorporation.
- Conduct adverse media checks and sanctions screening on the entity, its directors, and beneficial owners.

7.3 Shell Companies & Opaque Structures

The Company will not enter into a commercial relationship with:

- Shell companies that cannot demonstrate genuine business activity.
- Entities that refuse to disclose beneficial ownership information.
- Companies registered in secrecy jurisdictions where beneficial ownership verification is impossible.

7.4 High-Risk Business Clients

Businesses in industries with elevated ML risk (e.g. cryptocurrency exchanges, cash-intensive businesses, unlicensed money service businesses) will be subject to EDD and senior management approval.

---

8. Transaction Monitoring & Payment Controls

8.1 Accepted Payment Methods

AfriTech Bridge accepts the following payment channels:

- Mobile money (MTN Mobile Money, Airtel Money, and equivalent EAC services).
- Bank transfers (direct debit or wire transfer from verified bank accounts).

- Internationally recognised debit or credit cards (Visa, Mastercard) processed via vetted payment gateways.
- Authorised digital wallets integrated through regulated payment service providers.

The Company will NOT accept:
- Cash payments.
- Anonymous prepaid cards or vouchers.
- Cryptocurrency or virtual asset payments (unless a compliant, regulated gateway is introduced and this Policy is updated accordingly).
- Payments from third parties who are not the registered customer (without documented justification and additional due diligence).
- Payments channelled through unregulated or unlicensed money service businesses.

8.2 Transaction Thresholds & Monitoring Rules

The following monitoring rules apply across all platforms:

Rule	Threshold / Trigger	Action
Single large transaction	Any payment ≥ RWF 500,000 (≈ USD 400)	Flags for compliance review; source of funds verification
Rapid successive payments	Multiple payments within 48 hours totalling ≥ RWF 500,000	Flag as potential structuring (smurfing); hold pending review
Unusual geographic payment	Payment from a country not matching the registered user's stated location	Additional verification required
Failed payment retries	3+ failed payment attempts followed by a successful one	Flag for review
Third-party payment	Payment from an account not matching the customer's registered name	EDD and written justification required
Refund to different account	Refund requested to an account different from the original payment source	Senior approval required; possible STR
Dormant account reactivation	Account inactive > 12 months, then high-value transaction	Re-verify identity and rerun CDD

8.3 Payment Gateway Due Diligence

All payment service providers (PSPs) and payment gateways integrated with AfriTech Bridge platforms must:

- Be licensed and regulated by a competent financial regulator.
- Have documented, auditable AML/CFT programmes.
- Undergo due diligence by the Compliance Officer before integration.
- Be reviewed annually.

9. Suspicious Activity Recognition & Reporting

9.1 Indicators of Suspicious Activity

All staff must be familiar with common red flags. Suspicious activity may include, but is not limited to:

Learner / Individual Red Flags:
- Reluctance to provide identity documents or provision of obviously forged documents.
- Inconsistency between stated profession/income and the ability to pay for high-value programmes.
- Payment from multiple unrelated third parties for a single enrolment.
- Requesting unusual refund arrangements, especially to different accounts.
- Enrolling in and withdrawing from multiple courses without completing them, combined with irregular payment patterns.
- Use of multiple accounts or identities for the same person.

Corporate / Employer Red Flags:
- Company with no verifiable online presence or business activity.
- Unusual payment amounts for job postings or recruitment services.
- Beneficial ownership information withheld or inconsistent.
- Payment from a country unrelated to the stated business location.
- Pressure to complete the transaction quickly without standard verification.

Platform-Level Red Flags:
- The same IP address or device used to register multiple unrelated user accounts.
- Patterns consistent with structuring transactions to stay below monitoring thresholds.
- Co-ordinated account creation and payment activity suggesting an organised scheme.

9.2 Internal Reporting Procedure

When a staff member identifies or suspects suspicious activity, they must:

1. **Do not tip off** — Do not inform the customer that a report is being filed or that their account is under review. Tipping off is a criminal offence under Rwandan law.
2. **Document the concern** — Record the transaction details, nature of concern, customer information, and date of discovery.
3. **Submit an Internal Suspicious Activity Report (ISAR)** to the Compliance Officer within **24 hours** of the observation.
4. The Compliance Officer reviews the ISAR within **48 hours**.
5. If the suspicion is substantiated, an **External Suspicious Transaction Report (STR)** is submitted to the **Financial Intelligence Unit Rwanda (FIU-Rwanda)** within the timeframe required by law (not exceeding **3 business days**).
6. If urgent (suspected imminent terrorist financing or serious crime), the FIU is contacted immediately.

9.3 External STR Submission

STRs are submitted to:

Financial Intelligence Unit Rwanda (FIU-Rwanda)
Website: https://fiurwanda.gov.rw
Contact: As published on the FIU official portal

Reports must include all mandated fields under Rwandan AML law, including customer identification data, transaction details, accounts involved, and the reason for suspicion.

9.4 No Obligation to Freeze Without FIU Direction

Unless directed by the FIU or a court order, AfriTech Bridge will not unilaterally freeze customer accounts solely on the basis of an STR submission. Account restrictions may be applied as a precautionary measure where ongoing harm is reasonably anticipated, in consultation with the Compliance Officer and senior management.

---

10. Sanctions Screening & Politically Exposed Persons (PEPs)

10.1 Sanctions Obligations

AfriTech Bridge will not conduct business with, or process payments involving, any individual or entity that is:

- Listed on the **UN Security Council Consolidated Sanctions List**.
- Listed on the **OFAC Specially Designated Nationals (SDN) List** (United States).
- Listed on the **UK HM Treasury Financial Sanctions List**.
- Listed on the **EU Consolidated Sanctions List**.
- Listed on any applicable **Rwanda-specific sanctions designation**.

10.2 Screening Process

- All new customers (individual and corporate) are screened against the above lists at onboarding.
- Existing customers are re-screened periodically (at minimum quarterly) and whenever sanctions lists are updated.
- Screening is conducted using a vetted commercial screening tool or manual database checks where automated tools are not yet deployed.
- Any match — including fuzzy/partial name matches — triggers a hold and escalation to the Compliance Officer.

10.3 PEP Identification & Management

- Customers are asked at onboarding whether they are, or are closely associated with, a Politically Exposed Person.
- Self-declaration is supplemented by database checks against PEP lists in the screening tool.
- All confirmed PEPs or PEP associates are automatically subject to **Enhanced Due Diligence (EDD)** and require **senior management approval** before onboarding.
- PEP status does not automatically disqualify a customer but requires ongoing heightened scrutiny.

11. Record Keeping & Data Retention

11.1 Records to be Kept

AfriTech Bridge will maintain accurate, secure records of the following:

- All CDD and KYC documentation collected from customers.
- All KYB documentation collected from corporate clients.
- All transaction records, including date, amount, currency, payment method, and parties involved.
- All Internal Suspicious Activity Reports (ISARs).
- All External STRs submitted to the FIU.
- Responses and communications from the FIU or law enforcement.
- Sanctions and PEP screening results and outcomes.
- Staff AML training records.
- This Policy and all previous versions.

11.2 Retention Period

All AML-related records must be retained for a minimum of **five (5) years** from the date of the transaction, termination of the business relationship, or submission of the report — whichever is the latest. This aligns with the requirements of Rwandan AML law.

Records must be stored securely, with access restricted to authorised personnel only. Electronic records must be protected against tampering, loss, and unauthorised access.

11.3 Data Subject Rights

Retention of AML records may override data subject requests for deletion (right to erasure) under applicable data protection law where such retention is required by law.

12. Staff Training & Awareness

12.1 Training Obligations

All staff who have any customer-facing, financial, or compliance-related role are required to complete AML training. Training is mandatory and completion is tracked.

12.2 Training Programme

Training Type	Audience	Frequency
AML Induction Training	All new hires	Within 30 days of joining
Annual AML Refresher	All staff	Every 12 months
Role-Specific AML Training	Finance, Operations, Platform Product Teams	Upon role change or annually
Escalation & STR Procedures	All managers and the Compliance Officer	Annually
Policy Update Briefing	All staff	Upon every material policy revision

12.3 Training Content

Training programmes will cover, at minimum:

- The nature and techniques of money laundering and terrorist financing.
- AfriTech Bridge's legal and regulatory obligations.
- This Policy and supporting procedures.
- How to recognise suspicious activity and red flags specific to the Company's platforms.
- Internal reporting procedures and how to submit an ISAR.
- The legal obligation not to tip off subjects under investigation.
- Consequences — personal, legal, and organisational — of non-compliance.

12.4 Training Records

Completion records, including dates, names, roles, and training materials used, must be retained for at least five (5) years.

---

13. Compliance Officer & Governance

13.1 Designation

AfriTech Bridge designates a **Money Laundering Reporting Officer (MLRO)** / **Compliance Officer** who holds senior management responsibility for AML compliance across all platforms.

13.2 Responsibilities of the Compliance Officer

The Compliance Officer is responsible for:

- Maintaining and updating this Policy.
- Overseeing the day-to-day implementation of AML controls.
- Reviewing all Internal Suspicious Activity Reports (ISARs).

- Submitting Suspicious Transaction Reports (STRs) to the FIU-Rwanda.
- Maintaining liaison with the FIU, regulatory authorities, and law enforcement as required.
- Overseeing staff AML training.
- Conducting or commissioning the annual AML risk assessment.
- Reporting to senior management and the Board on AML compliance matters.
- Approving high-risk customer onboarding.
- Maintaining all AML records.

13.3 Board & Senior Management Responsibilities

The Board of Directors is ultimately accountable for AML compliance. Senior management shall:

- Approve this Policy and any material revisions.
- Allocate adequate resources (budget, staff, technology) to AML compliance.
- Review the Compliance Officer's annual AML report.
- Set a culture of compliance from the top.

13.4 Independence

The Compliance Officer must be able to act independently without commercial pressure or management interference in their AML functions. A direct reporting line to the Board is available where independence may be compromised.

---

14. Third-Party & Partner Due Diligence

14.1 Third-Party Reliance

Where AfriTech Bridge relies on a third party (e.g. a payment gateway, an identity verification provider, or an academic partner) to perform elements of CDD, the Company remains ultimately responsible for the adequacy of that due diligence.

14.2 Requirements for Third-Party Reliance

Before relying on a third party to perform CDD, AfriTech Bridge must satisfy itself that:

- The third party is subject to and compliant with AML/CFT obligations in their jurisdiction.
- The third party has adequate procedures in place.
- The third party will immediately provide CDD information upon request.
- The legal responsibility for CDD compliance is documented in the contractual agreement.

14.3 Outsourcing

The outsourcing of AML functions does not transfer legal liability. The Compliance Officer retains oversight of all outsourced AML activities.

---

15. Breach, Escalation & Whistleblowing

15.1 Internal Breach

Any breach of this Policy — whether by an employee, contractor, or agent — is a serious disciplinary matter. Breaches will be investigated promptly and may result in:

- Formal disciplinary action, up to and including termination of employment or contract.
- Referral to relevant law enforcement authorities.
- Civil and/or criminal liability for the individual concerned.

15.2 Whistleblowing

AfriTech Bridge encourages staff to report concerns about AML compliance without fear of retaliation. Staff may report concerns:

- Directly to the Compliance Officer.
- Via the Company's designated confidential reporting channel (to be established and communicated to all staff).
- Directly to the FIU-Rwanda if the staff member has reasonable grounds and the concern involves senior management.

The Company prohibits any retaliation, victimisation, or adverse treatment of any person who makes a good-faith report of an AML concern.

15.3 Reporting to Regulators

Where required by law, or where internal escalation is inadequate, the Compliance Officer may report regulatory breaches directly to the National Bank of Rwanda, the RIB, or the FIU, as appropriate.

---

16. Policy Review & Updates

16.1 Review Schedule

This Policy is reviewed at minimum **annually** by the Compliance Officer and approved by senior management. Ad hoc reviews will be triggered by:

- Material changes to the Company's business model, products, or services.
- Introduction of new payment methods or technology.
- Changes in applicable laws, regulations, or FATF standards.
- Identification of a significant AML incident or near-miss.
- Regulatory guidance or enforcement action in the EdTech or digital marketplace sector.

16.2 Version Control

All versions of this Policy will be version-controlled, dated, and archived. The current version will be made accessible to all staff.

17. Sign-Off & Approvals

Role	Name	Signature	Date
Compliance Officer / MLRO			
Chief Executive Officer			
Board of Directors (Chairperson)			

Appendix A: Glossary of Financial Crime Terms

Term	Definition
Placement	The first stage of money laundering: introducing illegal funds into the financial system.
Layering	The second stage: disguising the trail through complex transactions.
Integration	The third stage: reintroducing the laundered funds into the legitimate economy.
STR	Suspicious Transaction Report — formal report submitted to the FIU.
ISAR	Internal Suspicious Activity Report — internal document submitted to the Compliance Officer.
FATF	Financial Action Task Force — the global standard-setter for AML/CFT.
EAC	East African Community — the regional economic bloc to which Rwanda belongs.
FIU	Financial Intelligence Unit — Rwanda's competent authority for AML reporting.
OFAC	Office of Foreign Assets Control (US) — maintains a globally relevant sanctions list.
PEP	Politically Exposed Person — individual in a prominent public role.
KYC	Know Your Customer — identity verification of individuals.
KYB	Know Your Business — identity and verification of corporate entities.
CDD	Customer Due Diligence — overall process of understanding customers.
EDD	Enhanced Due Diligence — heightened checks for high-risk relationships.
SDD	Simplified Due Diligence — reduced checks for demonstrably low-risk relationships.

Appendix B: Key Contacts

Authority	Contact Details
FIU Rwanda	https://fiurwanda.gov.rw
National Bank of Rwanda (BNR)	https://www.bnr.rw
Rwanda Investigation Bureau (RIB)	https://rib.gov.rw
Rwanda Development Board (RDB)	https://rdb.rw
AfriTech Bridge Compliance Officer	[To be designated and communicated internally]
Confidential Whistleblowing Channel	[To be established and communicated to all staff]

Appendix C: Summary of Platform-Specific AML Controls

Control	LMS (study.afritechbridge.online)	Job Portal (jobs.afritechbridge.online)
KYC at enrolment / registration	Required before payment	Required for employers before posting
Payment methods accepted	Mobile money, card, bank transfer	Mobile money, card, bank transfer
Cash accepted	No	No
Cryptocurrency accepted	No	No
Transaction threshold for review	≥ RWF 500,000	≥ RWF 500,000
Third-party payments	EDD required	EDD required
PEP screening	Yes	Yes (especially employer-side)
Sanctions screening	Yes	Yes
Ongoing monitoring	Yes	Yes
Free programme exemption (SDD)	Yes (no funds flow)	N/A

This document constitutes the official Anti-Money Laundering Policy of AfriTech Bridge. It is confidential and intended for internal use. Unauthorised distribution outside the Company is prohibited except where required by law or regulatory authority.