# Anti-Money Laundering and Counter-Financing of Terrorism Policy

EaziWage

# Anti-Money and Counter-Financing of Terrorism Policy

## Version History

| Version No. | Date Updated | Updated By | Update Summary |
|---|---|---|---|
| 1 | 17 Oct 2025 | Jason Crawford | First AML and CFT Policy |

## Approval Record

| Version No. | Date Approved | Approved By |
|---|---|---|
| 1 | 17 Oct 2025 | EaziWage Holdings Limited Board Members |

## Ownership

Chief Executive Officer

## Applicability

The Anti-Money and Counter-Financing of Terrorism ("AML and CFT") Policy ("the Policy") applies to all employees, employers, contractors, agents, investors, banks and any other individuals or entities within the EaziWage Group, if and where relevant.

Failure to comply with these policies and procedures may result in disciplinary action, including but not limited to warnings, additional training, termination of employment, or legal action.

# 1. Anti-Money Laundering & Counter-Financing of Terrorism Policy Statement

EaziWage Holdings Limited ("the Firm") and its associated companies (the "Group") are fully committed to preventing the misuse of its operations, products, and services for the purposes of money laundering, terrorist financing, or other financial crimes.

The Firm maintains a **zero-tolerance stance** against financial crime and shall comply with all applicable Kenyan laws and regulations, including:

- **Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), No. 9 of 2009**
- **Proceeds of Crime and Anti-Money Laundering Regulations of 2013**
- **Prevention of Terrorism Act of 2012**
- **Guidelines issued by the Financial Reporting Centre (FRC)**
- **CBK Prudential Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism (CBK/PG/08)**

This policy aims to safeguard the integrity of the Firm's financial systems and reputation by establishing robust governance, controls, and compliance frameworks to detect, deter, and report money laundering or terrorism financing activities.

All employees, officers, directors, agents, and third-party partners must adhere to this policy.

# 2. Legal and Regulatory Framework

### 2.1 Applicable Laws and Regulations

This policy is grounded in Kenyan legislation, notably:

- **Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) of 2009** – criminalises money laundering and establishes obligations for reporting institutions.
- **Proceeds of Crime and Anti-Money Laundering Regulations of 2013** – detail compliance procedures, recordkeeping, and reporting requirements.
- **Prevention of Terrorism Act of 2012** – establishes offences relating to terrorism financing.

- **Financial Reporting Centre (FRC)** – established under Section 21 of POCAMLA as Kenya's financial intelligence unit (FIU), responsible for receiving, analysing, and disseminating suspicious transaction reports.
- **Central Bank of Kenya Prudential Guidelines (CBK/PG/08)** – applicable to institutions regulated by the CBK, setting out minimum AML/CFT requirements.

### 2.2 Definition of Money Laundering and Terrorism Financing

- **Money Laundering (Section 3, POCAMLA):** the process of concealing, disguising, converting, transferring, or dealing with the proceeds of crime to make them appear legitimate.
- **Terrorism Financing:** providing or collecting funds with the intention that they be used, or knowing they will be used, for terrorist acts.

Money laundering typically involves three stages:

1. **Placement** – introducing illicit funds into the financial system.
2. **Layering** – concealing the origin of funds through complex transactions.
3. **Integration** – reintroducing the laundered funds into the economy as apparently legitimate assets.

# 3. Objectives of the Policy

- Ensure full compliance with Kenyan AML/CFT laws and regulations.
- Protect the Firm and its customers from financial crime risks.
- Establish and maintain effective systems and internal controls for AML/CFT compliance.
- Promote staff awareness, accountability, and integrity in all dealings.
- Foster cooperation with regulatory and enforcement agencies, including the FRC, CBK, and law enforcement.

# 4. Roles and Responsibilities

### 4.1 Board of Directors and Senior Management

- Provide strategic oversight of AML/CFT compliance.
- Approve this Policy and ensure adequate resources for implementation.

- Review compliance reports, suspicious activity trends, and internal audit findings at least annually.
- Demonstrate top-level commitment to an ethical, compliant culture.

### 4.2 Chief Executive Officer

- Acts as the primary point of contact with the **Financial Reporting Centre (FRC)**.
- Receives and assesses internal Suspicious Transaction Reports (STRs).
- Ensures timely submission of STRs and Cash Transaction Reports (CTRs) to FRC.
- Maintains secure records of reports, investigations, and communications with authorities.
- Provides periodic AML/CFT training and reports to senior management.

### 4.3 Employees and Associated Persons

- Must understand and comply with this Policy and related procedures.
- Identify and report suspicious activity immediately to the Chief Executive Officer.
- Refrain from "tipping off" any person involved in a suspicious transaction.
- Participate in AML/CFT training sessions and awareness programs.

# 5. Customer Due Diligence (CDD)

### 5.1 General Requirements

Before establishing any business relationship or carrying out a transaction, the Firm shall:

- Identify and verify the customer's identity using reliable, independent source documents (e.g. National ID, Passport, Certificate of Incorporation, KRA Pin Certificate).
- Obtain information on the **purpose and intended nature** of the relationship.
- Identify and verify the **beneficial owner** (where applicable).
- Assess the **risk profile and/or credit risk** of the customer and transaction.

### 5.2 Enhanced Due Diligence (EDD)

Enhanced due diligence shall be applied to:

- High-risk customers (e.g. politically exposed persons (PEPs), foreign clients, complex structures).
- High-value or unusual transactions.

- Transactions or relationships involving jurisdictions with inadequate AML/CFT controls.

EDD measures may include obtaining senior management approval, verifying sources of funds, and closer ongoing monitoring.

### 5.3 Simplified Due Diligence (SDD)

SDD may be applied to low-risk customers (e.g. government agencies, regulated financial institutions) in accordance with FRC and CBK guidelines.

### 5.4 Ongoing Monitoring

- Monitor transactions to ensure consistency with the customer's profile and expected behaviour.
- Scrutinize complex, unusual, or large transactions with no apparent lawful purpose.
- Escalate any inconsistencies to the Chief Executive Officer for further investigation.

# 6. Record Keeping

In compliance with **Regulation 25 of the POCAMLA Regulations of 2013**, the Firm shall maintain:

- All CDD records and transaction documentation for **at least seven (7) years** after the end of the business relationship or transaction.
- STRs, CTRs, and internal reports securely for the same duration.
- Electronic or physical records that are easily retrievable and protected from unauthorized access or alteration.

# 7. Reporting Obligations

### 7.1 Suspicious Transaction Reports

- Employees must promptly report any suspicion of money laundering, terrorism financing, or related financial crimes to the Chief Executive Officer.
- The Chief Executive Officer will review and, if warranted, file an STR with the FRC within the prescribed timelines.
- It is a criminal offence under POCAMLA to fail to report suspicious activity.

### 7.2 Cash Transaction Reports

- The Firm shall submit CTRs to the FRC for all cash transactions exceeding the prescribed threshold (currently **KES 1,000,000** or its foreign currency equivalent).

### 7.3 Prohibition on Tipping-Off

No employee shall disclose or discuss with any person the fact that an STR or related report has been made or may be made. Breach of this obligation constitutes an offence under Section 48 of POCAMLA.

# 8. Risk Assessment

The Firm shall conduct an **AML/CFT risk assessment** annually and whenever there are material changes in operations, products, or markets. Risk factors include:

- **Customer risk** (nature of the customer, occupation, beneficial ownership).
- **Product/service risk** (ease of misuse for laundering).
- **Geographic risk** (jurisdictions with weak AML/CFT frameworks).
- **Delivery channel risk** (e.g. mobile or digital payments).

The Firm's compliance program shall allocate greater resources and controls to higher-risk areas and customers.

# 9. Training and Awareness

The Firm shall provide mandatory AML/CFT training for all employees upon joining and annually thereafter. Specialized training shall be provided to management, compliance teams, and front-line staff handling transactions or onboarding.

Training topics include red-flag indicators, customer due diligence, recordkeeping, and reporting procedures. Attendance and completion shall be recorded and monitored by the Chief Executive Officer.

# 10. Internal Controls  Independent Audit

- The Firm shall maintain written internal AML/CFT procedures, risk registers, escalation channels, and approval matrices.

- Internal audit shall independently review the AML/CFT program annually to assess its effectiveness and compliance with laws.
- Audit findings and corrective actions shall be reported to senior management and tracked to completion.

# 11. Cooperation with Authorities

The Firm will cooperate fully and in good faith with competent Kenyan authorities including the FRC, CBK, DPP, and law enforcement agencies.

- Information will be shared as permitted by law.
- The Firm will not obstruct or delay investigations and shall maintain confidentiality.

# 12. Penalties and Disciplinary Action

Violations of POCAMLA or this Policy may result in:

- Disciplinary action (including termination).
- Personal criminal liability (fines up to KES 5 million and/or imprisonment for up to 14 years).
- Corporate fines or sanctions. or
- Reporting to regulatory or law enforcement agencies.

# 13. Policy Review and Updates

This Policy shall be reviewed at least **annually** or upon significant regulatory or operational changes. Amendments will be approved by the Board of Directors and communicated to all staff.

All employees must acknowledge receipt and understanding of the latest version.

# Contact Us

info@eaziwage.com

+254 72 315 4900

EaziWage