Anti-Money Laundering (AML) Policy

ZIVEST (PTY) LTD

1. Purpose

The purpose of this Anti-Money Laundering (AML) Policy is to prevent ZIVEST (PTY) LTD from being used for money laundering, terrorist financing, or related financial crimes, and to support compliance with South African AML/CFT legal and regulatory requirements applicable to its activities.

---

2. Scope

This policy applies to:

- The Board of Directors
- Senior management
- Key Individuals and Representatives
- Employees and contractors
- All relevant products, services, customers, and transactions

---

3. Regulatory and Legal Framework

This policy is informed by applicable South African AML/CFT laws and supervisory standards to the extent that they apply to ZIVEST, including:

- The Financial Intelligence Centre Act (FICA) and related directives administered by the Financial Intelligence Centre
- AML/CFT supervisory and conduct requirements of the relevant authorities, including the Financial Sector Conduct Authority where applicable
- Relevant guidance notes, directives, and risk-based approach principles applicable to the company and its activities

4. AML Governance and Responsibilities

4.1 Board of Directors

The Board is responsible for:

- Approving the AML Policy and framework
- Providing oversight of AML/CFT risks
- Ensuring adequate resources, systems, and controls are in place
- Reviewing material AML issues, breaches, and regulatory communications

4.2 Senior Management

Senior management is responsible for:

- Implementing the AML framework
- Promoting a strong AML compliance culture
- Ensuring operational controls align with AML requirements
- Escalating material AML risks to the Board

4.3 Compliance Officer / Money Laundering Reporting Officer (MLRO)

The Compliance Officer (or designated MLRO) is responsible for:

- Maintaining the AML Policy and procedures
- Conducting AML risk assessments
- Monitoring compliance with FICA and related obligations
- Receiving and assessing internal suspicious transaction reports
- Submitting reports to the Financial Intelligence Centre where legally required
- Acting as the primary liaison with regulators

4.4 Employees

All employees must:

- Comply with AML policies and procedures
- Complete AML training
- Identify and report suspicious or unusual activity promptly
- Refrain from tipping off customers

---

5. Risk-Based Approach

ZIVEST (PTY) LTD applies a **risk-based approach** to AML/CFT, considering:

- Customer risk (e.g. individuals, corporates, foreign exposure)
- Product and service risk (investment-related activity, payment flows, and foreign-exchange transactions where applicable)
- Geographic risk
- Transaction and delivery channel risk

Enhanced controls are applied where higher risk is identified.

---

6. Customer Due Diligence (CDD)

6.1 Standard Due Diligence

Prior to establishing a business relationship, the company:

- Identifies and verifies customer identity
- Verifies beneficial ownership (where applicable)
- Understands the nature and purpose of the business relationship

6.2 Enhanced Due Diligence (EDD)

EDD is applied where higher risk exists, including:

- Politically Exposed Persons (PEPs)

- Complex ownership structures
- High-risk jurisdictions
- Unusual transaction behaviour

EDD measures may include senior management approval and additional verification.

6.3 Ongoing Due Diligence

- Customer information is kept up to date
- Transactions are monitored for consistency with the customer profile
- Periodic reviews are conducted based on risk rating

---

7. Transaction Monitoring

- Relevant transactions are monitored for unusual or suspicious patterns
- Thresholds and alerts are applied where appropriate
- Monitoring considers transaction size, frequency, destination, and behaviour

---

8. Suspicious and Unusual Transaction Reporting

- Employees must report suspicious or unusual activity internally to the MLRO immediately
- The MLRO assesses reports and submits:
    - Suspicious Transaction Reports (STRs)
    - Cash Threshold Reports (CTRs), where applicable
- All reporting is conducted confidentially and without tipping off customers

---

9. Record-Keeping

ZIVEST (PTY) LTD maintains AML records, including:

- Customer identification and verification documents
- Transaction records
- Internal and external AML reports
- Risk assessments and monitoring records

Records are retained in accordance with statutory retention periods and regulatory expectations.

---

10. Training and Awareness

- AML training is provided on induction and annually thereafter
- Training covers:
    - AML/CFT obligations
    - Red flags and suspicious behaviour
    - Reporting obligations and confidentiality
- Training attendance is documented and retained

---

11. Sanctions and PEP Screening

- Customers and transactions are screened against applicable sanctions lists
- PEP screening is conducted at onboarding and periodically thereafter
- Matches are escalated and assessed promptly

---

12. Breach Management

- AML breaches or control failures are escalated immediately
- Root causes are investigated and remedial actions implemented

- Material breaches are reported to regulators where required

---

13. Review and Continuous Improvement

- This policy is reviewed at least annually or following:
    - Legislative or regulatory changes
    - Material changes to business operations
    - Significant AML incidents
- The AML framework is enhanced based on regulatory feedback and internal findings

---

14. Policy Ownership and Approval

- **Policy Owner:** Compliance Officer / MLRO
- **Approved by:** Board of Directors
- **Effective Date: [To be confirmed by ZIVEST]**
- **Next Review Date: [To be confirmed by ZIVEST]**

Commitment Statement

ZIVEST (PTY) LTD is committed to maintaining robust AML/CFT controls to protect customers, comply with South African law, and safeguard the integrity of the financial system.