POLICIES AND PROCEDURES:
ANTI-MONEY LAUNDERING

1. INTRODUCTION

Creating a comprehensive Anti-Money Laundering (AML) policy for our company in South Africa and globally involves outlining a framework of procedures to prevent, detect, and respond to money laundering and financing of terrorism activities. The policies and procedures should comply with both South African regulations and international standards to ensure the highest level of financial and reputational integrity for the company.

1.1 Purpose

The purpose of this Anti-Money Laundering (AML) policy is to provide a detailed framework for the identification, prevention, and reporting of money laundering and terrorist financing activities at INTERVUSLATT . This policy outlines the approach, procedures, and measures to be followed by all employees, contractors, and third parties associated with the company

1.2 Legal Framework

This policy is designed in accordance with the following legal and regulatory requirements:

- The Financial Intelligence Centre Act (FICA) No. 38 of 2001 (South Africa)
- The Prevention of Organised Crime Act (POCA) No. 121 of 1998 (South Africa)
- The Terrorism Financing Act No. 33 of 2004 (South Africa)
- The Financial Action Task Force (FATF) Recommendations
- The United Nations Security Council Resolutions (UNSCR) regarding the sanctions on money laundering and terrorist financing
-International best practices and AML/CTF (Counter-Terrorist Financing) standards

2. AML GOVERNANCE FRAMEWORK

2.1 Appointment of Designated AML Officer

An Anti-Money Laundering Officer (AML Officer) will be appointed to oversee the implementation of the AML policy. The AML Officer will be responsible for:

- Ensuring compliance with this policy and applicable laws
- Monitoring transactions for suspicious activity
- Reporting suspicious transactions to the Financial Intelligence Centre (FIC)
- Overseeing employee training on AML issues
- Conducting regular audits of compliance processes

2.2 AML Committee

An AML Committee will be established to provide oversight and to review, monitor, and ensure adherence to the AML policies. The committee will meet quarterly to review the company's AML practices, procedures, and reports.

2.3 Risk-Based Approach

The company will apply a risk-based approach to AML compliance. This includes identifying high-risk customers, transactions, and regions to implement enhanced due diligence (EDD) where necessary.

3. KNOW YOUR CUSTOMERS PROCEDURE(KYC)

3.1 Customer Due Diligence (CDD)

Before entering into any business relationship, the company will conduct thorough Know Your Customer (KYC) checks, including:

- Verification of identity through official government-issued identification, including passport or national identity card.
- Verification of the customer's physical address through utility bills, bank statements, etc.
- For corporate clients: Verification of the company's registration, ownership structure, and identification of the beneficial owners (with at least a 25% stake in the business).

3.2 Enhanced Due Diligence (EDD)

For higher-risk clients, including those with connections to high-risk countries or industries (e.g., politically exposed persons (PEPs), or customers involved in high-value transactions), the company will implement Enhanced Due Diligence (EDD):

- Obtaining additional information about the client, such as source of wealth, purpose of the transaction, and business relationships.
- Ongoing monitoring of the client's transactions and relationship with the company.

3.3 Simplified Due Diligence (SDD)

Where the risks are deemed low, such as for certain low-value transactions or lower-risk sectors, the company may apply Simplified Due Diligence (SDD). However, SDD will never be applied to customers who are determined to be high-risk, such as PEPs.

4. ONGOING MONITORING OF CUSTOMERS AND TRANSACTIONS

4.1 Transaction Monitoring

- **Real-Time Monitoring**: Transactions will be continuously monitored using automated systems to detect unusual or suspicious activities (e.g., large transactions or transactions inconsistent with customer profiles).

- **Threshold Limits**: Transactions that exceed certain thresholds will trigger alerts for review by the AML Officer and further investigation.

- **Review of High-Value Transactions**: Each transaction above a specific threshold (e.g., R1,000,000) will be subject to further scrutiny, including a review of the source of funds and purpose of the transaction.

4.2 Periodic Reviews

Regular reviews of the customer's transactions, business relationships, and profiles will be conducted to ensure continued compliance with KYC and AML requirements. High-risk customers will be reviewed annually, while lower-risk customers may be reviewed every two years.

5. SUSPICIOUS ACTIVITY REPORTING

5.1 Reporting Suspicious Transactions

If any suspicious activity is detected, the AML Officer will assess the transaction and, if appropriate, file a Suspicious Transaction Report (STR) with the Financial Intelligence Centre (FIC).

- Suspicious activity could include: Unusual patterns, transactions that have no apparent economic or lawful purpose, or sudden unexplained activity in an otherwise dormant account.

5.2 Reporting to Law Enforcement

In cases where money laundering or terrorist financing is suspected, the company may also report incidents to the South African Police Service (SAPS) or other relevant authorities.

6. AML TRAINING AND AWARENESS

6.1 Employee Training Program

All employees, including the management team, will undergo mandatory AML training. The training will be held:

- Upon hiring
- Annually for all employees
- Upon significant updates to AML laws or refinery procedures

The training will cover:

- Basic understanding of money laundering and terrorist financing risks
- Recognizing red flags for suspicious transactions
- Reporting requirements under FICA and POCA
- The company's internal AML policies and procedures

6.2 Third-Party Training

All third-party service providers or contractors that engage in transactions on behalf of the company must also be trained on the AML policies and must adhere to similar standards.

7. RECORD KEEPING AND DOCUMENTATION

7.1 Record Retention

The company will retain all records relating to customer identification, transactions, and suspicious activity for a minimum of 5 years, in compliance with FICA and other relevant laws. These records will include:

- KYC and CDD records
- Transaction logs
- Suspicious activity reports (SAR)
- Communications related to AML compliance

7.2 Data Protection

All customer information and transaction records will be kept confidential and secure in line with data protection laws such as the Protection of Personal Information Act (POPIA).

8. INTERNAL CONTROLS AND AUDITING

8.1 Internal Audit Process

The company will implement an internal audit process to regularly review the effectiveness of the AML policy and procedures. Independent audits will be conducted annually, and any deficiencies or issues will be reported to the AML Committee for corrective action.

8.2 External Audits

External auditors will be engaged periodically to conduct an independent review of the company's AML compliance.

9. SANCTIONS AND PENALTIES

9.1 Non-Compliance

Failure to adhere to this AML policy will result in disciplinary action. Non-compliance may include:

- Suspension or termination of employees
- Suspension of business relationships
- Reporting to the relevant authorities for potential legal action

9.2 Regulatory Sanctions

The company acknowledges that failure to comply with AML regulations may result in penalties, including:

- Fines
- Imprisonment for individuals found guilty of money laundering or terrorist financing
- Revocation of operating licenses

10. AML POLICY REVIEW AND UPDATES

This AML policy will be reviewed and updated annually, or sooner if there are significant changes in South African legislation, international regulations, or business operations that necessitate adjustments to the policy.

The company commits to upholding the highest standards of AML compliance to protect its operations and contribute to the global fight against money laundering and terrorist financing. Through strict adherence to the above policies, robust systems for monitoring and reporting, and continuous training and auditing, the our company will ensure a secure and trustworthy business environment.