ANTI-MONEY LAUNDERING (AML) POLICY

1. OBJECTIVE

This policy outlines the Company's commitment to preventing and detecting money laundering activities and ensuring full compliance with applicable anti-money laundering (AML) regulations.

2. REGULATORY FRAMEWORK

The Company complies with the Anti-Money Laundering Act of 2014 and the Anti-Terrorism Act of 2007 of the Union of the Comoros (the "Acts"). These Acts aim to criminalize money laundering and deprive offenders of the profits from illicit activities.
To comply with these requirements, the Company has implemented robust policies and procedures, including, but not limited to:

- Client identification and due diligence measures.
- Record-keeping of client data and transaction details.
- Enhanced scrutiny of high-risk or unusual transactions.

3. CLIENT IDENTIFICATION AND DUE DILIGENCE

The Company enforces stringent identification and verification measures, such as:

- At the start of a business relationship.
- For single or linked transactions exceeding USD 15,000.
- When there is suspicion of money laundering or terrorist financing, irrespective of the transaction amount.
- If doubts arise regarding the accuracy of previously collected client information.

Verification of a client's identity is required prior to commencing a business relationship or executing transactions. Under limited circumstances, such as low risk of illicit activity, verification may be completed shortly after initial contact to avoid disrupting business operations.

Enhanced Due Diligence:
For high-risk situations, including politically exposed persons (PEPs) or clients not physically present, the Company applies heightened scrutiny and compensatory measures. As the Company does not accept face-to-face clients, enhanced procedures are standard practice.

Politically Exposed Persons (PEPs):
PEPs, individuals holding prominent public roles, or their close associates are subject to additional

checks. The Company prohibits opening or maintaining accounts in third-party names and diligently assesses attempts to use third-party accounts for illicit purposes.

4. RISK CATEGORIZATION

Clients are categorized into risk levels based on the likelihood of involvement in money laundering or terrorist financing:

- **Low Risk**: Individuals/entities with verifiable identities, consistent economic profiles, and transactions matching declared income.

- **Normal Risk**: Individuals/entities with verifiable identities and a transaction pattern aligned with their economic profile.

- **High Risk**: Clients posing higher-than-average risks, triggering enhanced due diligence. Refusal to provide required information without valid justification may result in the suspension of the relationship and reporting to the Financial Intelligence Unit (FIU).

5. RECORD-KEEPING

To comply with legal obligations, the Company retains comprehensive records for investigations or audits by national authorities, including:

- Client identification documents (e.g., passports, ID cards).
- Counterparty details (e.g., names, addresses).
- Transaction details (e.g., account numbers, payment instructions).
- Correspondence with clients.

Records are maintained for the legally mandated period and securely stored to prevent unauthorized access.