Marketvents Ltd

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy

1. Introduction, Purpose and Scope

Marketvents Ltd, trading as Marketvents (the "Company"), is incorporated in the Union of the Comoros under IBC number HV00726498, holds brokerage license no. BFX2026059 issued by the Mwali International Services Authority (MISA), and has its registered office at Bonovo Road, Fomboni, Island of Moheli, Comoros Union.

The Company issues this Policy to comply with the anti-money laundering and counter-terrorist financing ("AML/CFT") laws and regulations that apply to it.

The Company is committed to running its business in line with these requirements and with any amendments or regulatory developments that affect it. This Policy sets out the framework the Company uses to:

- prevent its products, services and trading accounts from being used for illicit purposes;
- identify and verify clients, beneficial owners and other relevant connected persons;
- assess and manage money laundering, terrorist financing and proliferation financing risks;
- identify politically exposed persons ("PEPs");
- screen clients and connected persons against applicable sanctions lists and other relevant watch-lists;
- identify adverse media and other reputational risk indicators;
- monitor business relationships and transactions on an ongoing basis;
- identify, escalate and report suspicious transactions;
- keep appropriate records; and
- train employees and responsible officers in their AML/CFT duties.

The Company follows a risk-based approach ("RBA"). This means that the depth of due diligence and monitoring applied to each client or relationship is proportionate to the risks identified.

This Policy is reviewed periodically and updated when needed to reflect changes in the Company's business, products and services, applicable law, regulatory expectations or emerging financial crime risks.

2. Definitions

- Money laundering – any conduct intended to conceal, disguise or obscure the unlawful origin, ownership, movement, destination or use of funds or other property derived from criminal activity, so that those assets appear legitimate. It includes acquiring, holding, using, transferring or converting property, or facilitating transactions involving property, that is known or reasonably suspected to be the proceeds of crime.

- Terrorist financing – providing or collecting funds or other assets, by any means, directly or indirectly, with the intention or knowledge that they will be used, in whole or in part, to carry out a terrorist act or by a terrorist or terrorist organization.
- Proliferation financing – providing funds or financial services for the manufacture, acquisition, transfer or use of nuclear, chemical or biological weapons and their means of delivery, in breach of national law or international obligations.
- AML/CFT – the laws, regulations, policies, procedures and internal controls designed to prevent, detect and respond to money laundering, terrorist financing and related financial crime.
- Predicate offence – any criminal offence that generates proceeds that can be laundered. This includes, at a minimum:
  (a) participation in organized crime;
  (b) terrorism and terrorist financing;
  (c) human trafficking and migrant smuggling;
  (d) sexual exploitation;
  (e) drug trafficking;
  (f) arms trafficking;
  (g) trafficking in stolen goods;
  (h) corruption and bribery;
  (i) fraud;
  (j) counterfeiting of currency and products;
  (k) environmental crime;
  (l) murder and serious bodily harm;
  (m) kidnapping and hostage-taking;
  (n) robbery and theft;
  (o) smuggling, including customs offences;
  (p) tax crimes;
  (q) extortion;
  (r) forgery;
  (s) piracy;
  (t) insider trading and market manipulation;
  (u) cybercrime; and
  (v) any other offence recognized as such under applicable law.
- Beneficial owner – the natural person(s) who ultimately own or control a client, or on whose behalf a transaction is carried out.
- PEP – a person who holds or has held a prominent public function in the Union of the Comoros, in another country or in an international organization, together with that person's family members and known close associates, as further defined in our Terms and Conditions.

3. Governance and Responsibilities

The Company maintains an AML/CFT framework designed to identify, assess, mitigate and monitor the financial crime risks arising from its activities and client relationships.

- The Board of Directors has ultimate responsibility for the effectiveness of the framework and approves this Policy and the Company's business-wide risk assessment at least once a year.
- Senior management ensures that appropriate risk management arrangements are developed and implemented and that the Board receives enough information on how well the AML/CFT controls are working.
- The Money Laundering Reporting Officer / Compliance Officer ("MLRO") is appointed by the Board and has the authority, independence, resources and direct access to the Board needed to carry out the role. The MLRO receives internal suspicion reports, decides whether external reports must be made, acts as the point of contact with the competent authorities and reports to the Board on AML/CFT matters at least annually. The MLRO may be supported by an outsourced compliance provider, but responsibility remains with the Company.
- All employees must understand and follow their AML/CFT responsibilities and receive appropriate training.

The Company's policies and procedures are reviewed regularly to ensure they remain suitable for its business model, products and services, client base, geographical markets and emerging money laundering, terrorist financing and other financial crime risks.

4. Core Controls

The Company takes a preventive approach. Its controls are designed to prevent its products and services from being used to:

- conceal or disguise the proceeds of crime;
- transfer or convert assets obtained illegally;
- facilitate criminal activity;
- hold assets derived from unlawful conduct; or
- otherwise circumvent applicable laws or regulatory requirements.

The Company will not knowingly accept funds, or start or continue a relationship, where there are reasonable grounds to believe that the assets involved come from unlawful activity or represent the proceeds of crime.

Clients must provide appropriate information and supporting documents about their identity and, where appropriate, about the source of funds and source of wealth behind their trading. AML/CFT controls are applied throughout the life of the relationship, not just at account opening.

4.1 Payment controls

To reduce the risk of misuse, the Company:

- does not accept cash deposits;
- accepts deposits only from accounts, cards or e-wallets held in the client's own name, and does not accept third-party payments except in the limited cases described in the Terms and Conditions and after additional checks;
- returns funds, as a rule, only to the same source and the same account from which they were received ("closed-loop" principle);
- may require evidence of ownership of a card or account (for example, a bank statement or card issuer letter) before crediting a deposit or paying a withdrawal; and
- reviews deposits that are followed by withdrawal requests with little or no trading activity, as this may indicate an attempt to use the trading account as a payment channel.

4.2 Prohibited relationships

The Company does not establish or maintain relationships with:

- anonymous persons or persons using fictitious names, and does not open anonymous or numbered accounts;
- shell banks, or entities whose ownership or control structure cannot be understood;
- persons or entities designated on any sanctions list applied by the Company;
- residents of jurisdictions subject to an FATF "call for action", or of any other jurisdiction listed as restricted in the Company's Terms and Conditions; and
- persons who refuse to provide the information or documents required for due diligence.

5. Customer Due Diligence (CDD)

The Company carries out CDD on prospective and existing clients to understand each client and the risks of the relationship. CDD is performed at onboarding and continues throughout the relationship.

CDD may take account of the following, among other factors:

- the client's identity (full legal name and date of birth);
- nationality and country of residence;
- occupation;
- the purpose and intended nature of the relationship;
- expected trading and transaction activity;
- source of funds ("SOF");
- source of wealth ("SOW");
- geographical location and exposure;
- PEP status;
- exposure to sanctions;
- adverse media; and
- any other factor that may affect the client's financial crime risk.

The Company always asks for identification documents and any other document it considers necessary to confirm the information above, such as a recent utility bill or bank statement. The information is verified using appropriate documents and, where necessary, independent and reliable sources. The Company may ask for additional information or documents at any time where needed to establish a client's identity, understand the relationship or manage an identified risk.

For corporate clients, the Company identifies the entity, verifies its legal existence and constitutional documents, understands its ownership and control structure, and identifies and verifies its directors, authorized signatories and beneficial owners.

No trading is permitted and no withdrawal is paid until verification has been completed to the Company's satisfaction. If verification cannot be completed, the Company will not open the account, or will close it, and will consider whether a suspicious transaction report is required.

6. PEP, Sanctions and Adverse Media Screening

As part of client acceptance and ongoing monitoring, the Company screens against relevant external and internal sources.

6.1 Politically exposed persons

The Company has procedures to determine whether a prospective or existing client, beneficial owner, authorised representative, director, shareholder or other connected person is a PEP. Screening is carried out at onboarding and repeated periodically or when the client's circumstances or risk profile change.

Where a PEP, or a person with similar political exposure, is identified, the Company assesses the risk and may apply enhanced due diligence and additional monitoring. It may ask for further information about the client's source of wealth, source of funds, business activities and the purpose of the relationship. Establishing or continuing a relationship with a foreign PEP requires senior management approval.

6.2 Sanctions

The Company screens clients and connected persons against applicable sanctions lists and other relevant restrictions.

Screening is carried out before the relationship begins and repeated during it on a risk-sensitive basis, as well as whenever sanctions lists or client information change. Potential matches are reviewed and investigated to determine whether they are true matches or false positives.

If a sanctions concern is confirmed, the Company takes appropriate action, which may include escalation, freezing of funds without delay, restriction or rejection of the relationship and/or transaction, and reporting to the competent authorities as required by the applicable framework.

6.3 Adverse media

The Company carries out reasonable adverse media screening to identify credible negative information about clients and connected persons, such as allegations or reports of money laundering, terrorist financing, fraud, corruption or other conduct that could materially increase financial crime or reputational risk. The Company assesses how credible, relevant, recent and serious the information is, and decides whether further due diligence or enhanced monitoring is appropriate.

7. Risk-Based Approach and Ongoing Monitoring

The Company assigns each client a risk rating based on its assessment. Factors include the client's country of residence and nationality, occupation and source of wealth, PEP status, the products used, payment methods, expected volumes and any adverse information. Higher-risk clients, transactions or relationships are subject to enhanced due diligence, closer monitoring and more frequent review.

Risk ratings are updated when new information becomes available or the client's activities or circumstances change.

The Company's monitoring obligation continues for the whole relationship. Accounts and transactions are monitored to detect activity that is inconsistent with the client's known profile, the stated purpose of the account, expected activity or other information the client has provided. Particular attention is paid to:

- complex or unusual transactions;
- unusually large transactions;
- unusual patterns of transactions;
- repeated smaller transactions that together may indicate suspicious activity (structuring);
- unexplained changes in behaviour;
- transactions inconsistent with the client's stated SOF;

- deposits and withdrawals with minimal trading activity;
- multiple accounts sharing the same device, IP address, payment method or personal details;
- geographical risk indicators; and
- activity with no apparent economic or lawful purpose.

8. Enhanced Due Diligence (EDD)

Where a client or relationship presents a higher risk of money laundering, terrorist financing or other financial crime, the Company applies EDD. EDD may include obtaining additional identification information, additional evidence of SOF and SOW, senior management approval of the relationship, more frequent monitoring and any other reasonable measure needed to reduce the risk identified.

EDD is always applied to PEPs, clients connected with high-risk jurisdictions (including those identified by the FATF as subject to increased monitoring), clients with complex ownership structures and any other client rated high-risk.

The Company may decline to start or continue a relationship where the risks cannot be adequately reduced or where the required information or documents cannot be obtained.

9. Suspicious and Large Transactions

The Company has procedures for identifying, assessing and escalating suspicious transactions and large or unusual transactions. Where a transaction or activity gives rise to reasonable grounds for suspicion, or meets a reporting threshold set by applicable law, the Company takes appropriate action and files the necessary report within the timeframe set by the applicable legislation or the competent authority.

The Company pays particular attention to transactions or patterns that are unusually complex or large, inconsistent with the client's known profile, repetitive without a legitimate purpose, inconsistent with the client's SOF, linked to high-risk jurisdictions or otherwise without an apparent lawful or economic purpose.

Monitoring takes into account transaction behaviour, source of funds and wealth, client risk indicators and geographical risk. The Company's approach is guided by the FATF Recommendations and other international standards on money laundering, terrorist financing and proliferation financing.

10. Internal Escalation and External Reporting

Employees must report any potentially suspicious activity to the MLRO promptly, using the internal reporting procedure. Employees discharge their legal duty by reporting to the MLRO. The MLRO reviews the matter and, where required, reports it to the competent authority – in the case of the Company, the Mwali International Services Authority and/or the Financial Intelligence Unit (Cellule de Renseignement Financier) of the Union of the Comoros, as applicable – in accordance with legal requirements.

Neither the MLRO nor any employee may tell a client or any third party that a report has been or may be made, or that an investigation is under way ("tipping-off"). The Company may restrict or suspend an account while a matter is being reviewed, without giving the reason.

The Company keeps records of investigations, decisions and reports relating to suspicious transactions – including decisions not to report and the reasons –. Employees must not knowingly facilitate any transaction or relationship that may involve the proceeds of crime or other unlawful activity.

11. Training

Relevant employees and officers receive AML/CFT training appropriate to their roles so that they can recognise and deal with AML/CFT risks. Training is given on joining and repeated at least once a year.

12. Record Keeping

The Company keeps appropriate records of its clients and their activities:

- transaction records are kept securely for at least five (5) years from the date of the transaction; and
- for closed accounts, client identification records, account files and relevant business correspondence are kept for at least five (5) years from the date of the relevant transaction or the end of the business relationship, as applicable.

Records are kept longer where an authority requires it or where they relate to an ongoing investigation, and are stored so that they can be made available promptly to the competent authorities on request.

13. Client Co-operation

By opening an account, clients agree to provide promptly any information or documents the Company reasonably requests for AML/CFT purposes. If a client fails to do so, the Company may decline instructions, suspend trading, withhold withdrawals until the request is satisfied, or close the account, as set out in the Terms and Conditions.

14. Review of this Policy

This Policy is reviewed periodically to confirm that it remains appropriate and effective. Where deficiencies or material changes are identified, the Company will update the Policy and/or its underlying procedures. The Company may amend this Policy at any time to keep it in line with the applicable legal and regulatory framework.