BOOXARO
YOUR EDGE, YOUR RULES, YOUR RESULTS.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM POLICY

SECTION 1: REGULATORY FRAMEWORK AND CORPORATE GOVERNANCE

1.1 This Anti-Money Laundering and Counter-Terrorism Policy (the "Policy") articulates the standards and procedures adopted by **BOOXARO** (the "Company," "we," "us," or "our") to prevent, identify, and address illicit financial activities, including, but not limited to, money laundering, terrorism financing, sanctions evasion, tax evasion, corruption, fraud, embezzlement, and other predicate offences as defined under applicable AML/CTF legislation.

1.2 The Company acknowledges and commits to full compliance with all applicable international and domestic legal requirements relating to ANTI-MONEY LAUNDERING (AML) and Counter-Terrorism Financing (CTF), retaining the authority to collaborate fully with regulatory bodies and law enforcement agencies upon reasonable suspicion of unlawful client conduct.

1.3 To maintain the integrity of its operations, the Company shall establish, enforce, and continuously enhance a robust compliance infrastructure comprising preventative controls, risk management processes, and ongoing evaluations designed to deter criminal misuse of its platform.

1.4 The Company adopts a strict zero-tolerance stance toward financial crimes of any nature. All personnel are required to uphold this Policy, with dedicated resources allocated for compliance training, supervision, and audit.

SECTION 2: CLIENT IDENTIFICATION AND DUE DILIGENCE

2.1 In alignment with Know Your Customer (KYC) obligations, all prospective and current clients must undergo comprehensive identity verification procedures. Clients consent to provide accurate, complete, and current personal and financial information as a prerequisite for engagement.

2.2 The Company mandates clients disclose the lawful origin of funds used in transactions, supported by appropriate documentary evidence, which shall be securely archived for auditing and regulatory compliance.

2.3 Disclosure of transaction records to third parties is restricted and shall only occur in accordance with statutory mandates and where such disclosure does not undermine investigative integrity or facilitate illegal activity.

2.4 Clients expressly authorize the Company to collect, process, and, when necessary, disclose relevant financial information to competent authorities, including the submission of Suspicious Transaction Reports (STRs), in full compliance with legal requirements.

2.5 Uniform verification standards shall apply equally to all clients, without exception or preferential treatment. The Company does not allow exceptions that could compromise regulatory adherence.

2.6 The Company reserves the right to assess the legal capacity of all clients, with the authority to terminate relationships where clients are determined legally incapable of entering into financial agreements.

SECTION 3: RISK ASSESSMENT AND TRANSACTIONAL CONTROLS

3.1 A risk-based framework guides the onboarding and continuous assessment of clients. Enhanced due diligence applies to high-risk clients, including Politically Exposed Persons (PEPs), individuals from high-risk jurisdictions, or those exhibiting suspicious behavior.

3.2 For clients assessed as low risk, streamlined due diligence may be employed consistent with regulatory standards. Risk categorization is subject to periodic review and adjustment.

3.3 The Company prohibits relationships with anonymous or fictitious entities. Transactions conducted via third parties require verifiable, legally valid power of attorney documentation.

3.4 The Company reserves the right to refuse, suspend, or terminate transactions or client accounts failing to meet the documentation and information requirements of this Policy.

3.5 Client risk evaluations shall consider business type, corporate structure, geographic factors, and transactional patterns. Engagements connected to terrorism financing or prohibited weaponry will prompt immediate account closure and reporting.

3.6 Regular internal audits and compliance reviews will be conducted to assess the effectiveness of AML/CTF protocols, incorporating transaction sampling, personnel assessments, and system integrity checks.

SECTION 4: MONITORING, RECORD RETENTION, AND ENFORCEMENT

4.1 The Company will continuously monitor client transactions and account activities using established internal benchmarks and external watchlists to identify and respond to anomalies or suspicious conduct.

4.2 All relevant records, including due diligence and transactional data, shall be maintained in accordance with regulatory retention periods and securely destroyed or anonymized thereafter.

4.3 Upon detection of suspicious activities, the Company shall promptly execute appropriate actions, such as account freezes, service suspensions, and statutory reporting to authorities.

4.4 Employees and representatives must report any known or suspected violations of this Policy. Whistleblower protections shall be upheld consistent with applicable laws.

4.5 The Company reserves the unilateral right to update or amend this Policy. Substantive modifications will be publicly announced, and continued use of the Company's services indicates acceptance of such changes.

4.6 This Policy shall be interpreted and enforced in accordance with prevailing AML and CTF laws. Non-compliance may result in account termination, legal reporting, and potential prosecution.

SECTION 5: TRAINING AND AWARENESS

5.1 The Company shall implement ongoing training programs to ensure all employees and agents are fully versed in AML and CTF legal requirements, internal procedures, and detection methodologies.

5.2 Training effectiveness will be periodically evaluated to ensure personnel readiness and adherence to this Policy.