RIT Gestion

Anti-money Laundering and Financial Crime Compliance Policy

CHAPTER I: GENERAL PROVISIONS

ARTICLE 1: PURPOSE AND REGULATORY SCOPE

1.1 This Anti-Money Laundering and Financial Crime Compliance Policy (the **"Policy"**) establishes the framework adopted by **RIT Gestion** (the **"Company," "we," "our," or "us"**) to identify, prevent, detect, assess, investigate, mitigate, and report money laundering, terrorist financing, sanctions violations, fraud, corruption, bribery, cyber-enabled financial crime, and other unlawful financial activities.

1.2 This Policy forms part of the Company's **Terms Governing Use of Services** and applies to Clients, prospective Clients, beneficial owners, authorized representatives, employees, contractors, agents, affiliates, service providers, and other persons or entities involved in the Company's Services, Trading Platforms, payment systems, or operational activities.

1.3 The Company shall maintain reasonable controls designed to support compliance with applicable AML, CTF, sanctions, anti-fraud, anti-corruption, and other financial crime prevention requirements.

1.4 The Company maintains a strict approach against the use of its Services for money laundering, terrorist financing, sanctions evasion, fraud, corruption, concealment of illicit proceeds, cyber-enabled financial crime, or other unlawful financial activity.

1.5 The Company may cooperate with financial intelligence units, regulators, governmental authorities, law enforcement agencies, sanctions authorities, courts, and other competent bodies where suspicious or unlawful activity is identified or reasonably suspected.

ARTICLE 2: INTERNAL COMPLIANCE FRAMEWORK

2.1 The Company may establish and maintain governance arrangements, compliance controls, transaction monitoring systems, due diligence procedures, sanctions screening, risk assessments, cybersecurity measures, audit mechanisms, and reporting procedures necessary to support this Policy.

2.2 The Company may reject an application, delay or refuse a transaction, restrict account functionality, suspend or terminate Services, freeze or withhold funds, delay withdrawals, or take other lawful measures where reasonably necessary due to suspected financial crime, sanctions exposure, incomplete verification, or other compliance concerns.

2.3 Directors, officers, employees, contractors, consultants, agents, and other personnel acting on behalf of the Company shall comply with applicable financial crime prevention requirements and internal compliance procedures.

2.4 The Company may allocate internal or external resources for compliance monitoring, employee training, sanctions screening, transaction surveillance, risk assessments, cybersecurity reviews, investigations, and regulatory reporting.

CHAPTER II: CLIENT IDENTIFICATION AND DUE DILIGENCE

ARTICLE 3: CLIENT IDENTIFICATION AND VERIFICATION

3.1 Before establishing a business relationship, activating relevant account functionality, processing certain transactions, or granting access to applicable Services, the Company may require completion of Customer Identification Program (**"CIP"**) and Know Your Customer (**"KYC"**) procedures.

3.2 Clients shall provide complete, accurate, current, and verifiable information concerning their identity, residency, nationality, financial profile, beneficial ownership, business activities, source of funds, source of wealth, and other information reasonably required for compliance purposes.

3.3 Verification documents may include:

(a) government-issued identification;

(b) passport or national identity documents;

(c) proof of residential address;

(d) corporate registration documents;

(e) beneficial ownership declarations;

(f) banking records;

(g) tax-related documents;

(h) source-of-funds evidence;

(i) financial statements; and

(j) other compliance documentation reasonably requested by the Company.

3.4 The Company may conduct identity verification, sanctions screening, politically exposed person (**"PEP"**) checks, adverse media screening, beneficial ownership reviews, database searches, biometric verification, and independent third-party due diligence.

3.5 The Company may collect, process, store, verify, transfer, and disclose Client information and compliance documentation where reasonably necessary for AML, CTF, sanctions, fraud prevention, cybersecurity, regulatory, or operational purposes, subject to applicable law and the Company's **Personal Data Governance and Security Policy**.

ARTICLE 4: ENHANCED DUE DILIGENCE

4.1 Enhanced Due Diligence (**"EDD"**) may be applied where a Client, transaction, jurisdiction, business relationship, or other circumstance presents elevated legal, financial, operational, reputational, or regulatory risk.

4.2 EDD measures may include:

(a) senior management approval;

(b) additional source-of-wealth or source-of-funds verification;

(c) enhanced transaction monitoring;

(d) continued sanctions screening;

(e) additional identity authentication;

(f) independent compliance investigations; and

(g) periodic reassessment of the Client's risk profile.

4.3 Anonymous accounts, fictitious identities, concealed beneficial ownership arrangements, and shell entities lacking a legitimate commercial purpose are prohibited.

4.4 The Company may reject, delay, restrict, suspend, or terminate an account or business relationship where verification is incomplete, information is inaccurate or misleading, fraud is suspected, regulatory concerns arise, or applicable compliance requirements are not satisfied.

4.5 Clients shall promptly notify the Company of material changes affecting their identity, beneficial ownership, residency, source of funds, source of wealth, legal status, or other information relevant to ongoing compliance requirements.

4.6 Failure to provide requested information or cooperate with due diligence procedures may result in delayed transactions, restricted account functionality, withdrawal delays, suspension of Services, or termination of the Client relationship where reasonably necessary.

CHAPTER III: RISK ASSESSMENT AND TRANSACTION CONTROLS

ARTICLE 5: RISK-BASED ASSESSMENT

5.1 The Company applies a risk-based approach (**"RBA"**) to identifying, assessing, categorizing, monitoring, and managing financial crime risks associated with Clients, transactions, jurisdictions, products, payment methods, and business relationships.

5.2 Risk assessments may consider:

(a) geographic location;

(b) nationality or residency;

(c) sanctions exposure;

(d) source of funds and source of wealth;

(e) transaction patterns;

(f) ownership structures;

(g) PEP status;

(h) adverse media;

(i) industry or business sector;

(j) use of intermediaries or third parties; and

(k) previous compliance concerns.

5.3 Relationships or activities involving terrorism financing, sanctions violations, proliferation financing, organized crime, cybercrime, corruption, bribery, trafficking, or other unlawful conduct may be subject to enhanced review, restrictions, suspension, termination, or reporting to competent authorities where required.

ARTICLE 6: TRANSACTION MONITORING AND CONTROLS

6.1 The Company may maintain transaction monitoring, behavioral analysis, sanctions screening, surveillance, and other control systems designed to identify unusual activity, suspicious transactions, financial crime indicators, sanctions exposure, and regulatory concerns.

6.2 Monitoring may consider transaction frequency, trading and payment patterns, deposits, withdrawals, geographic inconsistencies, IP addresses, device information, payment routing, account relationships, movement of funds, and other relevant activity.

6.3 The Company may investigate, delay, reject, restrict, suspend, reverse, or freeze a transaction pending completion of compliance, fraud, operational, or regulatory review where reasonably necessary.

6.4 Transactions involving third parties may be subject to enhanced scrutiny and may require valid authorization documents, powers of attorney, corporate approvals, beneficial ownership information, or other evidence reasonably requested by the Company.

6.5 The Company may decline transactions or relationships involving jurisdictions, institutions, entities, individuals, industries, or activities considered prohibited, sanctioned, high-risk, or incompatible with its compliance obligations.

CHAPTER IV: REPORTING AND INFORMATION MANAGEMENT

ARTICLE 7: SUSPICIOUS ACTIVITY AND REGULATORY REPORTING

7.1 Where suspicious activity or conduct is identified or reasonably suspected, the Company may submit Suspicious Transaction Reports (**"STRs"**), Suspicious Activity Reports (**"SARs"**), sanctions notifications, or other reports to competent authorities where required or permitted by applicable law.

7.2 The Client acknowledges that the Company may be legally prohibited from disclosing the existence, nature, status, or outcome of an investigation, monitoring activity, or regulatory report.

7.3 The Company may restrict account access, freeze or withhold funds, suspend Services, delay withdrawals, restrict transactions, or implement other safeguards where reasonably necessary to address suspected financial crime, sanctions exposure, fraud, or regulatory concerns.

7.4 Employees, contractors, consultants, and other relevant personnel shall report known or suspected violations of this Policy through the Company's designated internal reporting channels.

7.5 The Company may maintain appropriate confidentiality and non-retaliation safeguards for personnel who report suspected misconduct in good faith, subject to applicable law and internal procedures.

ARTICLE 8: RECORD RETENTION AND INFORMATION MANAGEMENT

8.1 The Company shall maintain appropriate records relating to Client identification, due diligence, transactions, communications, compliance reviews, investigations, and regulatory reporting for the periods required by applicable law, regulatory standards, and internal procedures.

8.2 Records may be maintained electronically, digitally, physically, or through secure archival systems and may be disclosed to regulators, auditors, financial intelligence units, law enforcement agencies, compliance providers, or other competent authorities where legally required or permitted.

8.3 The Company may preserve, analyze, review, and use relevant records for compliance, investigative, regulatory, audit, cybersecurity, legal, operational, and evidentiary purposes.

CHAPTER V: TRAINING AND COMPLIANCE OVERSIGHT

ARTICLE 9: PERSONNEL TRAINING AND AWARENESS

9.1 The Company shall maintain appropriate training and awareness measures designed to ensure that relevant personnel understand AML, CTF, sanctions, fraud prevention, cybersecurity, suspicious activity indicators, reporting requirements, and applicable internal procedures.

9.2 Training may include onboarding programs, periodic refresher training, compliance testing, sanctions awareness, cybersecurity education, operational exercises, risk assessments, and regulatory updates.

9.3 The Company may assess personnel understanding and compliance through audits, testing, supervisory reviews, monitoring activities, and other internal assessment procedures.

ARTICLE 10: COMPLIANCE MONITORING AND ENFORCEMENT

10.1 The Company may periodically review and assess the effectiveness of its financial crime prevention framework and introduce additional controls where risks, regulatory developments, or operational circumstances require.

10.2 Non-compliance with this Policy may result in account restrictions, transaction limitations, suspension or termination of Services, regulatory reporting, recovery actions, legal proceedings, or other measures permitted under applicable law.

10.3 The Company may conduct internal investigations or engage external legal, compliance, audit, cybersecurity, or other professional advisers where reasonably necessary to address financial crime concerns.

CHAPTER VI: FINAL PROVISIONS

ARTICLE 11: POLICY AMENDMENTS

11.1 The Company may amend, supplement, revise, replace, suspend, withdraw, or otherwise modify this Policy where reasonably required by changes in law, regulatory expectations, financial crime risks, technology, cybersecurity threats, operational requirements, or business circumstances.

11.2 Unless otherwise stated, amendments shall become effective upon publication through the Company's Official Website, Client Portal, Trading Platform, or another authorized communication channel.

11.3 Continued access to or use of the Company's Services following publication of amendments shall constitute acknowledgment and acceptance of the revised Policy.

ARTICLE 12: LEGAL EFFECT AND CONTINUING OBLIGATIONS

12.1 This Policy forms a binding supplementary part of the Company's **Terms Governing Use of Services** and shall be interpreted consistently with applicable laws, regulatory requirements, sanctions obligations, and lawful directions issued by competent authorities.

12.2 Nothing in this Policy restricts the Company's ability to comply with applicable law, cooperate with competent authorities, conduct lawful investigations, or implement measures reasonably necessary to protect its operations and compliance framework.

12.3 If any provision of this Policy is determined to be invalid, unlawful, or unenforceable, the remaining provisions shall continue in effect to the fullest extent permitted by applicable law.

12.4 Obligations relating to record retention, confidentiality, investigations, regulatory reporting, enforcement, and other matters that by their nature require continuing effect shall remain applicable following account termination or cessation of the Client relationship.