RIT Gestion

Personal Data Governance and Security Policy

CHAPTER I: GENERAL PROVISIONS

ARTICLE 1: PURPOSE AND SCOPE

1.1 This Personal Data Governance and Security Policy (the **"Policy"**) establishes the principles and safeguards applied by RIT Gestion (the **"Company," "we," "us," or "our"**) in relation to the collection, use, processing, storage, disclosure, transfer, retention, and protection of personal, financial, technical, and other information handled through the Company's Services and digital infrastructure.

1.2 This Policy forms part of the Company's **Terms Governing Use of Services** and applies to Clients, prospective Clients, authorized representatives, beneficial owners, visitors, contractors, service providers, operational partners, and other persons whose information is processed by the Company in connection with its Services.

1.3 The Company seeks to maintain appropriate confidentiality, integrity, availability, and lawful handling of information through reasonable administrative, organizational, technical, operational, and cybersecurity safeguards.

1.4 Information may be processed electronically, digitally, manually, automatically, internally, or through authorized third-party providers where required for contractual, legal, regulatory, operational, or compliance purposes.

1.5 By accessing or continuing to use the Company's Services, the Client acknowledges that they have reviewed and accepted the practices and requirements established under this Policy.

ARTICLE 2: INFORMATION GOVERNANCE AND INTERNAL CONTROLS

2.1 The Company may establish and maintain internal procedures, access controls, cybersecurity measures, monitoring systems, audit processes, compliance frameworks, and other safeguards designed to protect information and maintain operational integrity.

2.2 The Company may conduct internal reviews, compliance assessments, fraud-prevention procedures, cybersecurity evaluations, and technical inspections where reasonably necessary to:

(a) protect information and systems;

(b) comply with applicable law;

(c) prevent unauthorized activity;

(d) investigate suspicious conduct; or

(e) maintain operational security.

2.3 Employees, officers, contractors, consultants, affiliates, agents, and authorized representatives who have access to information shall remain subject to applicable confidentiality, security, and information-handling requirements.

2.4 The Company may engage internal or external resources for cybersecurity, compliance, fraud prevention, risk management, infrastructure protection, audits, monitoring, and employee training.

2.5 The Company may cooperate with regulators, financial institutions, law enforcement agencies, governmental authorities, cybersecurity specialists, and other authorized parties where disclosure or cooperation is legally required or reasonably necessary for legitimate operational, security, or compliance purposes.

CHAPTER II: INFORMATION COLLECTION AND PROCESSING

ARTICLE 3: PERSONAL INFORMATION AND VERIFICATION

3.1 The Company may collect, verify, process, maintain, and store personal, financial, technical, and operational information during account registration, onboarding, transaction processing, compliance reviews, fraud prevention, cybersecurity monitoring, and Service administration.

3.2 Information collected may include:

(a) legal name, date and place of birth, nationality, and citizenship;

(b) residential or mailing address;

(c) telephone number and email address;

(d) government-issued identification and passport information;

(e) banking and payment details;

(f) employment and financial information;

(g) tax-related information;

(h) technical device identifiers; and

(i) other information reasonably required for legal, regulatory, operational, or security purposes.

3.3 The Company may request additional information or documentation to satisfy KYC, AML, CTF, sanctions, fraud-prevention, cybersecurity, and regulatory requirements.

3.4 Verification materials may include identification documents, proof of address, bank statements, corporate records, beneficial ownership information, source-of-funds or source-of-wealth evidence, tax residency information, and other documents reasonably required for compliance purposes.

3.5 The Company may use internal systems, sanctions databases, fraud-prevention tools, cybersecurity technologies, and authorized third-party verification services to verify identity, assess risk, and satisfy applicable legal and regulatory requirements.

ARTICLE 4: AUTOMATED COLLECTION AND TECHNICAL INFORMATION

4.1 The Company may automatically collect technical, analytical, behavioral, operational, and transactional information generated through the Client's interaction with the Website, Trading Platforms, applications, and Services.

4.2 Such information may include:

(a) IP address;

(b) browser and operating system information;

(c) device identifiers;

(d) access and login information;

(e) session activity;

(f) geolocation indicators;

(g) clickstream and usage information;

(h) transaction patterns;

(i) device fingerprinting information; and

(j) other technical analytics.

4.3 This information may be collected through cookies, server logs, analytics tools, cybersecurity systems, monitoring technologies, and fraud-prevention software for purposes including authentication, system maintenance, service improvement, fraud prevention, security, compliance, and operational administration.

4.4 The Company may combine technical information with personal, financial, or transactional information where reasonably necessary for fraud detection, cybersecurity, compliance, operational security, service improvement, or other lawful business purposes.

CHAPTER III: INFORMATION SECURITY AND RETENTION

ARTICLE 5: SECURITY MEASURES AND ACCESS PROTECTION

5.1 The Company shall implement commercially reasonable measures intended to protect information against unauthorized access, misuse, disclosure, alteration, destruction, compromise, or unlawful processing.

5.2 Security measures may include:

(a) encryption technologies;

(b) Secure Socket Layer (**"SSL"**) protocols;

(c) multi-factor authentication (**"MFA"**);

(d) access controls;

(e) firewalls;

(f) intrusion detection and threat monitoring;

(g) cybersecurity surveillance;

(h) incident response procedures; and

(i) internal security assessments.

5.3 The Company may require additional authentication, identity verification, account recovery checks, or enhanced security procedures where unusual activity, suspected compromise, or other security concerns arise.

5.4 The Client acknowledges that no electronic system, network, storage environment, or cybersecurity framework can guarantee complete protection against cyberattacks, unauthorized access, interception, malicious software, technical failures, or other security threats.

ARTICLE 6: RETENTION AND DISPOSAL OF INFORMATION

6.1 The Company may retain personal information, verification records, transaction data, communications, operational logs, account records, and compliance documentation for periods reasonably necessary to:

(a) perform contractual obligations;

(b) comply with legal and regulatory requirements;

(c) resolve disputes;

(d) prevent fraud;

(e) conduct cybersecurity or operational investigations; or

(f) protect the Company's legitimate interests.

6.2 Following expiry of the applicable retention period, the Company may securely delete, anonymize, archive, destroy, or otherwise dispose of information in accordance with applicable law and internal security procedures.

6.3 Information may be retained beyond ordinary periods where reasonably necessary for regulatory investigations, legal proceedings, fraud prevention, cybersecurity assessments, compliance reviews, audits, or enforcement actions.

CHAPTER IV: USE AND DISCLOSURE OF INFORMATION

ARTICLE 7: AUTHORIZED PROCESSING AND THIRD-PARTY SERVICES

7.1 Personal information may be processed for legitimate contractual, operational, legal, regulatory, compliance, cybersecurity, fraud-prevention, and business administration purposes.

7.2 Processing activities may include:

(a) account administration;

(b) Service delivery;

(c) identity verification;

(d) transaction processing;

(e) customer support;

(f) fraud prevention;

(g) cybersecurity monitoring;

(h) operational analysis;

(i) compliance monitoring;

(j) legal enforcement;

(k) internal audits; and

(l) regulatory reporting.

7.3 The Company may engage affiliates, payment processors, technology providers, cloud service providers, cybersecurity specialists, compliance partners, contractors, and other authorized service providers to perform functions on its behalf.

7.4 Information shared with such parties shall remain subject to applicable confidentiality, security, contractual, and legal requirements.

ARTICLE 8: LEGAL DISCLOSURES AND INTERNATIONAL TRANSFERS

8.1 The Company may disclose personal information where reasonably necessary to comply with applicable laws, court orders, governmental directives, regulatory requirements, supervisory requests, compliance investigations, or lawful enforcement actions.

8.2 The Company shall not disclose one Client's personal information to another Client except where required or permitted by applicable law, judicial proceedings, arbitration, regulatory requirements, or lawful enforcement procedures.

8.3 The Client acknowledges that information may be processed, stored, transferred, or accessed outside their country of residence where reasonably necessary for:

(a) cloud hosting;

(b) payment processing;

(c) operational continuity;

(d) compliance administration;

(e) cybersecurity;

(f) technical support; or

(g) other lawful business purposes.

8.4 The Company shall use commercially reasonable safeguards intended to maintain appropriate confidentiality, security, and compliance standards when information is transferred internationally.

CHAPTER V: CLIENT RIGHTS AND AUTOMATED PROCESSING

ARTICLE 9: DATA SUBJECT RIGHTS

9.1 Subject to applicable legal, regulatory, operational, and compliance requirements, the Client may request:

(a) access to their personal information;

(b) correction of inaccurate information;

(c) restriction of certain processing;

(d) withdrawal of marketing consent; or

(e) deletion of personal information where legally permissible.

9.2 Requests for deletion or restriction may be refused or delayed where continued processing or retention is reasonably necessary for AML compliance, fraud prevention, dispute resolution, legal proceedings, cybersecurity investigations, contractual enforcement, or regulatory obligations.

9.3 The Client may object to certain processing activities where permitted by applicable law, particularly where processing is based primarily on operational, analytical, commercial, or marketing interests rather than a mandatory legal obligation.

9.4 The Company may continue processing where overriding legal, regulatory, cybersecurity, fraud-prevention, operational, or legitimate business grounds apply.

9.5 Subject to identity verification and applicable legal restrictions, the Client may request certain personal information in a structured electronic format where such disclosure is reasonably feasible.

9.6 The Company may withhold, redact, restrict, or refuse disclosure where necessary to protect cybersecurity measures, confidential systems, third-party rights, fraud-prevention activities, legal obligations, or regulatory interests.

9.7 The Company may distribute service-related, compliance, educational, operational, or promotional communications through electronic channels. The Client may withdraw

consent for promotional communications without affecting the underlying contractual relationship.

ARTICLE 10: AUTOMATED PROCESSING AND DECISION-MAKING

10.1 The Company may use automated systems, algorithmic tools, fraud detection technologies, risk assessment models, transaction monitoring systems, and cybersecurity analytics for compliance, security, fraud prevention, account monitoring, transaction review, and operational purposes.

10.2 Automated assessments may contribute to decisions concerning:

(a) account verification;

(b) transaction reviews;

(c) enhanced due diligence;

(d) withdrawal restrictions;

(e) account suspension;

(f) fraud-prevention measures; or

(g) operational risk management.

10.3 Where reasonably appropriate and legally permissible, the Company may conduct additional human review before implementing material restrictions or enforcement measures arising from automated assessments.

CHAPTER VI: CYBERSECURITY AND INCIDENT RESPONSE

ARTICLE 11: SECURITY MONITORING AND THREAT RESPONSE

11.1 The Company may maintain cybersecurity monitoring, threat detection, vulnerability assessments, penetration testing, intrusion prevention, surveillance, and incident response systems designed to protect the Platform, Client information, internal systems, and associated infrastructure.

11.2 Where cybersecurity threats, unauthorized access, malicious activity, technical vulnerabilities, or data compromise risks are identified or reasonably suspected, the Company may temporarily suspend, isolate, delay, restrict, or terminate access to an account, transaction, communication channel, Platform function, or system.

11.3 Following an actual or suspected security incident, the Company may take reasonable measures to investigate, contain, and mitigate the incident, including:

(a) account suspension;

(b) password resets;

(c) enhanced identity verification;

(d) transaction restrictions;

(e) access revocation;

(f) forensic investigation; and

(g) emergency security controls.

ARTICLE 12: INCIDENT NOTIFICATION AND CLIENT SECURITY

12.1 Where required by applicable law, regulation, or operational necessity, the Company may notify affected Clients, financial institutions, cybersecurity specialists, regulators, law enforcement authorities, or other relevant parties of a cybersecurity or information security incident.

12.2 The timing and content of any notification may be affected by legal restrictions, investigative confidentiality, security considerations, containment measures, and regulatory requirements.

12.3 The Client remains responsible for protecting passwords, login credentials, authentication devices, email accounts, access codes, and other communication channels associated with their account.

12.4 The Client shall promptly notify the Company of suspected unauthorized access, compromised credentials, phishing attempts, suspicious communications, malware exposure, or other security incidents affecting their account or devices.

12.5 To the extent permitted by applicable law, the Company shall not be liable for losses arising from the Client's failure to maintain reasonable account, device, credential, or cybersecurity safeguards.

CHAPTER VII: FINAL PROVISIONS

ARTICLE 13: THIRD-PARTY RESOURCES AND SECURITY REVIEWS

13.1 The Platform may contain links, integrations, or access points to third-party websites, applications, software, or services operated independently of the Company.

13.2 The Company does not control and shall not be responsible for the privacy practices, cybersecurity measures, content, or operational standards of independent third-party platforms.

13.3 The Company may periodically conduct operational reviews, cybersecurity assessments, penetration tests, compliance evaluations, risk audits, and internal investigations to strengthen its information governance and security framework.

ARTICLE 14: PRIVACY REQUESTS AND LEGAL EFFECT

14.1 Requests concerning personal information access, correction, privacy complaints, consent withdrawal, security concerns, or compliance matters shall be submitted through the Company's designated communication channels.

14.2 For security and verification purposes, the Company may require requests to originate from the Client's registered email address or another verified communication channel.

14.3 The Client shall comply with reasonable verification requirements before the Company processes a request concerning personal information or account security.

14.4 The Company may amend, replace, supplement, suspend, or update this Policy where reasonably required for legal, regulatory, operational, cybersecurity, technological, or commercial purposes.

14.5 Continued use of the Services following publication of amendments shall constitute acknowledgment and acceptance of the revised Policy.

14.6 Nothing in this Policy limits any rights, remedies, powers, or obligations available to the Company under applicable law or contractual arrangements.

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