CAPITAL NOMOS

AML, CTF, AND FINANCIAL CRIME PREVENTION POLICY

1. REGULATORY FRAMEWORK AND CORPORATE GOVERNANCE

1.1 Scope, Purpose, and Regulatory Commitment

1.1.1 This AML, CTF, and Financial Crime Prevention Policy *(the "Policy")* is adopted and implemented by **CAPITAL NOMOS** *(hereinafter referred to as the "Company," "we," "us," or "our")* for the purpose of establishing a comprehensive compliance framework designed to detect, prevent, deter, investigate, monitor, mitigate, and report activities associated with money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption, bribery, tax evasion, cyber-enabled financial crime, embezzlement, identity theft, unlawful enrichment, concealment of illicit proceeds, and other forms of prohibited financial conduct under applicable laws, regulations, directives, and internationally recognized compliance standards.

1.1.2 This Policy shall operate as a supplementary and legally binding component of the Company's Conditions of Use and shall apply to all Clients, prospective Clients, authorized representatives, beneficial owners, affiliates, agents, contractors, employees, and all individuals or entities accessing or utilizing the Company's Services, Trading Platforms, payment systems, software infrastructure, digital interfaces, and operational environments.

1.1.3 The Company is committed to maintaining compliance with all applicable Anti-Money Laundering *("AML")*, Counter-Terrorist Financing *("CTF")*, sanctions compliance, anti-corruption, anti-bribery, fraud prevention, and financial crime prevention obligations arising under applicable domestic legislation, international conventions, financial intelligence requirements, and regulatory frameworks.

1.1.4 The Company may cooperate with financial intelligence units, supervisory authorities, regulatory bodies, sanctions enforcement agencies, governmental institutions, law enforcement authorities, judicial entities, and international compliance organizations where unlawful conduct, suspicious activity, sanctions violations, terrorism financing concerns, or financial crime indicators are identified or reasonably suspected.

1.1.5 The Company maintains a strict zero-tolerance approach toward money laundering, terrorism financing, sanctions evasion, financial fraud, corruption, unlawful concealment of assets, cyber-enabled financial crime, misuse of financial systems, or conduct intended to facilitate illicit financial activity.

1.2 Corporate Compliance Obligations and Internal Governance

1.2.1 The Company shall establish, implement, maintain, and continuously enhance internal governance structures, compliance controls, operational safeguards, transaction monitoring systems, due diligence procedures, cybersecurity measures, audit mechanisms, and risk management frameworks intended to identify, prevent, and mitigate financial crime exposure.

1.2.2 The Company may, where reasonably necessary and consistent with applicable legal and regulatory obligations, reject onboarding applications, delay or refuse transactions, suspend services, terminate accounts, restrict operational access, freeze balances, delay withdrawals, or report activity to competent authorities in circumstances involving suspected unlawful conduct, sanctions exposure, compliance concerns, operational risk, or suspicious activity.

1.2.3 All officers, directors, employees, contractors, consultants, operational personnel, and representatives of the Company shall remain subject to the obligations contained within this Policy and shall comply fully with all AML, CTF, sanctions screening, fraud prevention, and compliance obligations established herein.

1.2.4 The Company may allocate internal and external resources for compliance oversight, employee education, sanctions screening, operational monitoring, transaction surveillance, cybersecurity review, risk assessment procedures, and regulatory reporting activities necessary to support implementation and enforcement of this Policy.

1.2.5 Nothing contained within this Policy shall restrict the Company's ability to comply with applicable laws, cooperate with competent authorities, fulfill regulatory obligations, or

undertake lawful measures reasonably necessary for the protection of its operational integrity, legal interests, and compliance responsibilities.

2. CLIENT IDENTIFICATION AND DUE DILIGENCE

2.1 Customer Identification and Verification Standards

2.1.1 All prospective and existing Clients shall, prior to establishing a business relationship, activating account functionality, processing transactions, or obtaining access to the Company's Services, undergo Customer Identification Program *("CIP")* procedures and Know Your Customer *("KYC")* verification measures implemented by the Company.

2.1.2 Clients shall provide accurate, complete, current, verifiable, and lawful information relating to their identity, residency, nationality, financial profile, beneficial ownership structure, business activities, source of wealth, source of funds, and all other information reasonably requested by the Company for compliance purposes.

2.1.3 Verification documentation required by the Company may include, without limitation:
(a) Government-issued identification documents;
(b) Passports or national identity cards;
(c) Proof of residential address;
(d) Corporate registration records;
(e) Beneficial ownership declarations;
(f) Banking documentation;
(g) Tax records;
(h) Source-of-funds evidence;
(i) Financial statements; and
(j) Additional compliance documentation deemed reasonably necessary by the Company.

2.1.4 The Company may conduct enhanced verification procedures, biometric authentication, database screening, sanctions screening, politically exposed person ("PEP") assessments, adverse media checks, beneficial ownership investigations, and independent third-party due diligence reviews at any stage of the Client relationship where reasonably necessary for compliance or risk management purposes.

2.1.5 Clients expressly acknowledge and consent to the Company collecting, storing, analyzing, processing, transferring, verifying, and disclosing personal information, financial records, account activity, and compliance documentation for AML, CTF, sanctions compliance, fraud prevention, cybersecurity, operational integrity, and regulatory reporting purposes in accordance with applicable laws and the Company's internal policies.

2.2 Enhanced Due Diligence and Compliance Reviews

2.2.1 The Company may apply Enhanced Due Diligence *("EDD")* procedures to Clients classified as presenting elevated legal, operational, financial, reputational, or regulatory risk.

2.2.2 Enhanced Due Diligence procedures may include:
(a) Senior management approval requirements;
(b) Additional source-of-wealth verification;
(c) Independent compliance investigations;
(d) Enhanced transaction monitoring;
(e) Ongoing sanctions screening;
(f) Additional identity authentication procedures; and
(g) Periodic reassessment of risk exposure.

2.2.3 Anonymous accounts, fictitious identities, shell entities lacking legitimate commercial purpose, or relationships involving concealed beneficial ownership structures are strictly prohibited.

2.2.4 The Company may reject, delay, suspend, terminate, or restrict account functionality where:
(a) Verification procedures remain incomplete;
(b) Documentation is inaccurate or misleading;
(c) Fraudulent activity is reasonably suspected;
(d) Regulatory concerns are identified; or
(e) The Client fails internal compliance review requirements.

2.2.5 Clients shall promptly notify the Company of any material changes relating to identity information, beneficial ownership, residency status, financial circumstances, source of wealth, source of funds, legal status, or operational activity relevant to ongoing compliance obligations.

2.2.6 Failure to comply with verification obligations, due diligence procedures, or ongoing compliance requests may result in delayed transactions, restricted account functionality, frozen balances, suspension of services, or termination of the Client relationship, where reasonably necessary for legal, regulatory, or operational purposes.

3. RISK ASSESSMENT AND TRANSACTIONAL CONTROLS

3.1 Risk-Based Compliance Methodology

3.1.1 The Company applies a risk-based approach *("RBA")* in assessing, categorizing, monitoring, and managing financial crime exposure associated with Clients, transactions, jurisdictions, products, payment methods, business relationships, and operational activities.

3.1.2 Risk evaluations may consider, without limitation:
(a) Geographic location;
(b) Citizenship or residency status;
(c) Sanctions exposure;
(d) Source of wealth and source of funds;
(e) Transactional behavior;
(f) Corporate ownership structures;
(g) Politically Exposed Person *("PEP")* status;
(h) Adverse media exposure;
(i) Industry sector;
(j) Use of intermediaries or Third Parties; and
(k) Historical compliance concerns.

3.1.3 Relationships involving terrorism financing, sanctions violations, weapons proliferation, organized crime, cybercrime, corruption, bribery, trafficking activities, or unlawful financial conduct may result in compliance escalation, enhanced review procedures, account

restriction, suspension of services, and regulatory reporting obligations where required under applicable law.

3.2 Transactional Monitoring and Operational Controls

3.2.1 The Company shall implement transaction monitoring systems, behavioral analysis mechanisms, sanctions screening controls, surveillance procedures, and operational review frameworks designed to identify suspicious activity, unusual transactional behavior, financial crime indicators, sanctions exposure, or regulatory breaches.

3.2.2 Monitoring activities may include review of transaction frequency, trading behavior, deposit patterns, withdrawal requests, geographic inconsistencies, IP address analysis, payment routing activity, device linkage, account relationships, liquidity movement, and unusual financial conduct.

3.2.3 The Company may investigate, delay, reject, restrict, suspend, reverse, or freeze transactions pending completion of compliance review, fraud analysis, operational verification, or regulatory reporting obligations where reasonably necessary for compliance, legal, or operational purposes.

3.2.4 Transactions initiated through Third Parties shall remain subject to additional scrutiny and may require legally valid authorization documents, including notarized powers of attorney, corporate authorizations, or beneficial ownership disclosures.

3.2.5 The Company may decline to process transactions or maintain business relationships involving jurisdictions, institutions, industries, entities, or individuals deemed high-risk, sanctioned, prohibited, or incompatible with the Company's compliance obligations or operational risk management standards.

4. MONITORING, RECORD RETENTION, AND ENFORCEMENT

4.1 Reporting, Surveillance, and Regulatory Cooperation

4.1.1 Where suspicious conduct is identified or reasonably suspected, the Company may file Suspicious Transaction Reports *("STRs")*, Suspicious Activity Reports *("SARs")*, sanctions notifications, or other regulatory reports with competent authorities in accordance with applicable legal and regulatory obligations.

4.1.2 Clients acknowledge that the Company may be prohibited by law from disclosing the existence of investigations, surveillance procedures, monitoring activities, regulatory reporting obligations, or compliance review processes.

4.1.3 The Company may freeze balances, suspend services, terminate accounts, restrict transactions, delay withdrawals, or implement operational safeguards where reasonably necessary in circumstances involving suspicious activity, sanctions exposure, fraud indicators, regulatory obligations, or unlawful conduct.

4.1.4 Employees, contractors, operational personnel, consultants, and representatives shall promptly report known or suspected violations of this Policy through designated internal reporting channels.

4.1.5 The Company shall implement appropriate whistleblower protections, confidentiality safeguards, and non-retaliation measures consistent with applicable laws, regulatory obligations, and internal compliance procedures.

4.2 Record Retention and Information Management

4.2.1 The Company shall maintain records relating to identification documents, due diligence materials, transactional activity, communications, compliance reviews, operational investigations, and reporting activities for such retention periods as required under applicable laws, regulatory standards, and internal compliance procedures.

4.2.2 Records retained pursuant to this Policy may be stored electronically, digitally, physically, or through secure archival systems and may be disclosed to regulators, auditors, compliance partners, financial intelligence units, law enforcement agencies, or competent authorities where legally required.

4.2.3 The Company may preserve, analyze, review, and utilize operational records, transaction histories, surveillance information, communication records, and compliance documentation for investigative, regulatory, operational, cybersecurity, audit, legal, and evidentiary purposes in accordance with applicable laws and internal procedures.

5. TRAINING, AWARENESS, AND COMPLIANCE OVERSIGHT

5.1 Internal Compliance Programs and Personnel Training

5.1.1 The Company shall establish and maintain ongoing compliance education and operational training programs designed to ensure that employees, officers, contractors, agents, consultants, and operational personnel remain adequately informed regarding AML, CTF, sanctions compliance, fraud prevention, cybersecurity risk, suspicious activity indicators, reporting obligations, and internal compliance procedures.

5.1.2 Training programs may include onboarding education, periodic refresher sessions, operational simulations, compliance testing, sanctions awareness programs, cybersecurity education, risk assessments, and regulatory update briefings.

5.1.3 The Company may evaluate personnel understanding, operational readiness, procedural compliance, and adherence to this Policy through internal audits, supervisory assessments, testing procedures, monitoring activities, and operational reviews.

5.2 Policy Enforcement, Amendments, and Continuing Obligations

5.2.1 The Company may amend, supplement, revise, replace, update, or enhance this Policy from time to time in response to evolving legal obligations, regulatory developments, operational requirements, technological advancements, cybersecurity threats, financial crime trends, or business considerations.

5.2.2 Continued access to or use of the Company's Services following publication or implementation of amendments to this Policy shall constitute acceptance of such modifications.

5.2.3 Non-compliance with this Policy may result in account suspension, transaction restrictions, service termination, regulatory reporting, legal proceedings, recovery actions, financial penalties, or other remedial measures reasonably necessary under applicable law.

5.2.4 The provisions of this Policy shall survive account termination, service discontinuation, or cessation of the business relationship to the extent necessary for regulatory compliance, investigations, enforcement proceedings, legal obligations, or operational protection of the Company.