

AML Due Diligence Policy

INTRODUCTION

The **AML Due Diligence Policy** (the “Policy”) establishes the framework through which the Company identifies, assesses, monitors, and manages risks relating to money laundering, terrorist financing, sanctions violations, fraud, tax evasion, corruption, and other forms of financial crime.

The Policy sets out the due diligence, identification, verification, risk assessment, monitoring, enhanced review, reporting, and recordkeeping measures applied by the Company when establishing and maintaining business relationships.

The Company applies a risk-based approach under which the nature, extent, and frequency of due diligence and monitoring may vary according to the risks associated with an Account Holder, beneficial owner, transaction, jurisdiction, business relationship, or other relevant circumstance.

This Policy applies to Account Holders, prospective Account Holders, beneficial owners, Authorized Persons, legal entities, and other individuals or entities seeking to establish or maintain a business relationship with the Company.

Compliance with this Policy forms part of the conditions governing access to the Company’s Services. The Account Holder acknowledges that the Company may request information or documentation, conduct reviews, restrict activity, suspend services, or take other measures where necessary to satisfy its legal, regulatory, compliance, and financial crime prevention obligations.



CHAPTER I: AML GOVERNANCE AND DUE DILIGENCE

PRINCIPLES

SECTION I.I: PURPOSE AND APPLICATION

The Company maintains controls designed to prevent, detect, deter, investigate, and respond to activities that may involve financial crime.

These controls are intended to support compliance with applicable anti-money laundering (“AML”), counter-terrorist financing (“CTF”), sanctions, fraud prevention, and other financial crime requirements.

The Company may introduce additional controls or verification measures where required by Applicable Law, regulatory expectations, internal risk assessments, or circumstances affecting the integrity or security of its operations.

This Policy shall apply throughout the relevant business relationship and shall not be limited to the initial account-opening or onboarding process.

SECTION I.II: RISK-BASED COMPLIANCE FRAMEWORK

The Company applies a risk-based approach to the identification, assessment, monitoring, and management of financial crime risks.

The level of due diligence and monitoring applied to an Account Holder may vary according to factors including geographic location, occupation, business activity, transaction patterns, source of funds, source of wealth, ownership structure, political exposure, and other relevant risk indicators.



The Company may revise an Account Holder's risk classification at any time where new information, changes in activity, regulatory developments, transaction patterns, or other circumstances indicate that the applicable risk assessment should be reconsidered.

SECTION I.III: ACCOUNT HOLDER COOPERATION

The Account Holder shall provide accurate, complete, current, and verifiable information and documentation whenever reasonably requested by the Company for identification, verification, due diligence, monitoring, or compliance purposes.

The Account Holder shall cooperate with the Company's compliance procedures throughout the business relationship and shall promptly notify the Company of material changes affecting previously submitted information.

Failure to satisfy applicable due diligence or compliance requirements may result in transaction restrictions, processing delays, enhanced review, suspension of Services, account closure, or other measures permitted under Applicable Law and the Company's governing documents.

CHAPTER II: IDENTIFICATION AND CUSTOMER DUE DILIGENCE

SECTION II.I: IDENTITY VERIFICATION AND ONBOARDING

The Company shall apply appropriate identification and verification procedures before establishing a business relationship or permitting access to its Services, subject to Applicable Law and the Company's risk-based procedures.

The Account Holder shall provide information reasonably required to establish and verify identity, residency, legal status, ownership, and other relevant characteristics.



The Company may request supporting documentation to verify information provided during onboarding or at any subsequent stage of the business relationship.

Where satisfactory verification cannot be completed, the Company may refuse, delay, restrict, suspend, or terminate the relevant application or business relationship.

SECTION II.II: KNOW YOUR CUSTOMER REQUIREMENTS

The Company maintains Know Your Customer (“KYC”) procedures designed to establish the identity of Account Holders and understand the nature and purpose of the relevant business relationship.

KYC procedures may include the collection and verification of identification documents, proof of address, source of funds information, source of wealth information, corporate records, ownership documentation, and other supporting materials.

The Company may conduct ongoing KYC reviews and require updated information or documentation throughout the duration of the business relationship.

The Account Holder shall promptly provide updated information where previously submitted information has materially changed or is no longer accurate.

SECTION II.III: SOURCE OF FUNDS AND SOURCE OF WEALTH

The Company may require an Account Holder to provide information concerning the origin of funds deposited with the Company and, where appropriate, the source of wealth supporting the Account Holder’s financial activities.



Evidence may include bank statements, employment records, business records, tax documentation, payment records, declarations, or other information reasonably required to establish the legitimacy and origin of funds or wealth.

Where the source of funds or source of wealth cannot be satisfactorily established, the Company may reject deposits, delay or restrict transactions, request further information, or take other appropriate compliance measures.

Failure to provide satisfactory evidence may result in restrictions on the account or termination of the business relationship.

SECTION II.IV: LEGAL CAPACITY AND ACCOUNT ELIGIBILITY

An Account Holder must possess the legal capacity and authority required to enter into binding arrangements with the Company and use its Services.

Where an Account Holder is a legal entity, partnership, trust, foundation, or other organization, the Company may require evidence of legal existence, ownership structure, beneficial ownership, management authority, and the authority of persons acting on its behalf.

The Company may decline an application or restrict an existing relationship where applicable legal capacity, eligibility, ownership, or compliance requirements cannot be satisfactorily established.

SECTION II.V: BENEFICIAL OWNERSHIP AND AUTHORIZED PERSONS

The Company shall take reasonable measures to identify and verify beneficial owners and persons exercising control over relevant legal entities or arrangements where required.



An individual acting on behalf of an Account Holder must provide documentation sufficient to establish their authority to do so.

The Company may require powers of attorney, corporate resolutions, authorization documents, trust documentation, or other legal evidence where a representative or other Authorized Person acts on behalf of an Account Holder.

The Company may refuse or restrict arrangements where the identity or authority of the relevant person cannot be adequately verified.

SECTION II.VI: ANONYMOUS, FICTITIOUS AND UNVERIFIED RELATIONSHIPS

The Company does not permit anonymous accounts, fictitious identities, or business relationships where the identity of the Account Holder or beneficial owner cannot be adequately established and verified.

The Company may restrict or prohibit transactions involving unidentified third parties, nominees, intermediaries, or arrangements that may materially increase financial crime or compliance risks.

Where sufficient information cannot be obtained to establish the parties involved in a business relationship or transaction, the Company may refuse to establish or continue the relationship.

CHAPTER III: RISK ASSESSMENT AND TRANSACTION MONITORING

SECTION III.I: ACCOUNT HOLDER RISK PROFILING

The Company may establish and maintain risk profiles for Account Holders to support its compliance and financial crime prevention framework.

Risk assessments may consider, among other factors:

- country of residence or incorporation;
- nature and purpose of the business relationship;
- occupation or business activities;
- anticipated and actual transaction volume;
- source of funds and source of wealth;
- beneficial ownership and control structures;
- political exposure;
- transaction patterns; and
- other indicators relevant to financial crime risk.
-

The Company may classify Account Holders according to different levels of risk and apply corresponding controls and monitoring measures.

SECTION III.II: TRANSACTION AND ACCOUNT MONITORING

The Company may monitor account activity, deposits, withdrawals, transfers, transactions, and other financial activity to identify unusual, suspicious, inconsistent, or potentially unlawful conduct.



Monitoring may be performed through automated systems, manual reviews, compliance investigations, or a combination of these methods.

The Company may request explanations, supporting documents, or additional information concerning activity that appears unusual or inconsistent with the Account Holder's known profile or expected activity.

Transactions may be delayed, restricted, rejected, or subjected to further review where the Company considers such action necessary for compliance, security, or risk-management purposes.

SECTION III.III: ONGOING DUE DILIGENCE

The Company may conduct periodic and event-driven reviews of Account Holder information, account activity, risk classifications, ownership structures, and supporting documentation.

The Company may request updated identification documents, source of funds information, source of wealth evidence, corporate records, declarations, or other materials as part of an ongoing review.

Additional due diligence may be applied where changes in circumstances, transaction activity, risk indicators, regulatory developments, or other factors indicate an increased level of financial crime risk.

Failure to cooperate with ongoing due diligence may result in account restrictions, suspension of Services, rejection of transactions, or termination of the business relationship.



SECTION III.IV: INTERNAL COMPLIANCE OVERSIGHT

The Company may maintain internal controls, monitoring systems, compliance testing, audit procedures, risk assessments, staff training, and other measures designed to support its AML and financial crime prevention framework.

Internal oversight may include transaction reviews, sanctions screening, compliance assessments, risk classification reviews, control testing, and independent or internal audits where appropriate.

The Company may modify or strengthen its compliance framework in response to changes in Applicable Law, regulatory requirements, emerging financial crime risks, or operational circumstances.

Nothing in this Policy shall restrict the Company from taking immediate protective or compliance action where it reasonably identifies a material financial crime or regulatory concern.

CHAPTER IV: ENHANCED DUE DILIGENCE AND HIGH-RISK RELATIONSHIPS

SECTION IV.I: ENHANCED DUE DILIGENCE

The Company may apply Enhanced Due Diligence (“EDD”) where an Account Holder, transaction, business relationship, jurisdiction, or activity presents an elevated level of money laundering, terrorist financing, sanctions, fraud, or other financial crime risk.



EDD measures may include additional identity verification, source of funds verification, source of wealth assessment, transaction analysis, management approval, increased monitoring, and requests for supplementary documentation or explanations.

The extent and duration of EDD measures shall be determined according to the Company's risk assessment procedures and applicable compliance requirements.

SECTION IV.II: POLITICALLY EXPOSED PERSONS

The Company may determine whether an Account Holder, beneficial owner, Authorized Person, family member, or close associate qualifies as a Politically Exposed Person ("PEP") where relevant to its compliance obligations.

An individual identified as a PEP may be subject to EDD and increased monitoring.

The Company may request additional information concerning the individual's public functions, source of wealth, source of funds, business activities, and related financial arrangements.

PEP status alone shall not necessarily prevent the establishment or continuation of a business relationship. However, additional controls may be applied where required by the Company's risk assessment or Applicable Law.

SECTION IV.III: HIGH-RISK JURISDICTIONS

The Company may classify countries, territories, or regions as presenting elevated financial crime or compliance risks based on applicable sanctions, regulatory guidance, financial crime indicators, corruption risks, political instability, or other relevant considerations.



Account Holders connected to higher-risk jurisdictions may be subject to additional verification, transaction monitoring, documentation requirements, and EDD.

The Company may restrict, suspend, decline, or terminate a business relationship involving a jurisdiction where the associated compliance, legal, regulatory, or financial crime risks are considered unacceptable.

SECTION IV.IV: SANCTIONS SCREENING

The Company may conduct sanctions screening against Account Holders, beneficial owners, Authorized Persons, counterparties, and other relevant individuals or entities.

The Company may refuse, restrict, suspend, terminate, or otherwise prohibit a relationship or transaction involving a person, entity, organization, vessel, jurisdiction, or other party appearing on an applicable sanctions list or subject to relevant restrictions.

The Company may take immediate action where it reasonably identifies a potential connection to sanctioned activity, prohibited transactions, restricted jurisdictions, terrorist organizations, criminal enterprises, or other unlawful conduct.

The Company shall not be required to provide advance notice where disclosure of such action is restricted or prohibited by Applicable Law or compliance requirements.

SECTION IV.V: PROHIBITED AND RESTRICTED RELATIONSHIPS



The Company may decline or discontinue a business relationship where an Account Holder is unable or unwilling to satisfy applicable identification, verification, due diligence, or compliance requirements.

The Company may refuse to establish or maintain relationships involving anonymous persons, fictitious identities, prohibited entities, sanctioned parties, or activities presenting unacceptable legal, regulatory, compliance, reputational, or operational risks.

Additional documentation or clarification may be required where concerns arise regarding ownership structures, transaction activity, source of funds, source of wealth, or other relevant compliance matters.

Measures taken under this Policy shall be without prejudice to any other rights available to the Company under its General Terms and Conditions or Applicable Law.

SECTION IV.VI: ENHANCED MONITORING

Business relationships assessed as presenting elevated risk may be subject to increased monitoring, more frequent reviews, enhanced transaction analysis, and additional compliance controls.

The frequency, scope, and duration of enhanced monitoring shall be determined according to the Company's risk assessment framework and applicable requirements.

The Company may reclassify an Account Holder and adjust applicable monitoring measures where transaction patterns, circumstances, regulatory developments, or other risk indicators change.



Enhanced monitoring may remain in place for as long as the Company considers it necessary to manage the identified risks.

CHAPTER V: REPORTING, CONFIDENTIALITY AND ENFORCEMENT

SECTION V.I: SUSPICIOUS ACTIVITY REVIEW AND REPORTING

The Company may investigate transactions, account activity, business relationships, or other conduct that it reasonably considers potentially connected to money laundering, terrorist financing, sanctions violations, fraud, or other financial crime.

Where required by Applicable Law, regulatory obligations, or internal compliance procedures, the Company may submit Suspicious Transaction Reports ("STRs"), Suspicious Activity Reports ("SARs"), or other required disclosures to competent authorities.

The Company shall not be required to notify the Account Holder of an investigation, review, report, disclosure, or communication made to a regulatory, supervisory, governmental, or law enforcement authority where such notification is prohibited or restricted.

The Company may delay, restrict, suspend, reject, or refuse transactions while relevant compliance reviews or investigations are ongoing.

SECTION V.II: CONFIDENTIALITY AND NON-DISCLOSURE



An Account Holder shall not be entitled to information concerning confidential internal investigations, compliance reviews, sanctions assessments, suspicious activity reports, regulatory disclosures, or other protected compliance activities.

The Company may withhold information where disclosure could compromise an investigation, regulatory obligation, crime prevention measure, legal proceeding, or compliance activity.

Nothing in this Policy shall require the Company to disclose confidential compliance methodologies, internal risk assessment procedures, monitoring systems, investigative techniques, or other protected information.

SECTION V.III: COMPLIANCE RECORDS

The Company may maintain records relating to Account Holder identification, verification, due diligence, transaction activity, communications, risk assessments, investigations, compliance reviews, and regulatory reporting.

Records may be maintained in physical, electronic, digital, or other appropriate formats.

Compliance records may be used for regulatory reporting, audits, investigations, dispute resolution, legal proceedings, risk management, internal controls, and other legitimate compliance purposes.

Records shall be retained for periods required by Applicable Law, regulatory obligations, internal policies, or legitimate business requirements.



The Company may retain relevant records following the closure or termination of a business relationship where necessary to satisfy continuing legal, regulatory, audit, compliance, or risk-management obligations.

SECTION V.IV: COMPLIANCE ENFORCEMENT MEASURES

The Company may take any action reasonably necessary to satisfy its AML, CTF, sanctions, financial crime prevention, legal, and regulatory obligations.

Such measures may include enhanced reviews, requests for additional information or documentation, transaction restrictions, account suspension, refusal of Services, termination of the business relationship, freezing or holding of transactions where permitted by Applicable Law, and reporting to competent authorities.

To the extent permitted by Applicable Law, the Company shall not be responsible for losses, delays, restrictions, or other consequences arising from actions taken in good faith to satisfy compliance obligations or manage identified financial crime risks.

SECTION V.V: CONTINUING ACCOUNT HOLDER COOPERATION

The Account Holder shall cooperate fully with reasonable requests for information, documentation, explanations, declarations, or other materials required for compliance purposes.

Failure to provide requested information within the timeframe specified by the Company may result in restrictions on account activity, suspension of Services, rejection of transactions, or termination of the business relationship.



The Account Holder acknowledges that compliance requirements may require information to be obtained or updated periodically throughout the business relationship and are not limited to the initial onboarding process.

CHAPTER VI: POLICY GOVERNANCE AND INTERPRETATION

SECTION VI.I: POLICY AMENDMENTS AND UPDATES

The Company may amend, revise, supplement, replace, or otherwise update this Policy where it considers such action necessary or appropriate for legal, regulatory, operational, compliance, technological, risk-management, or business purposes.

An amended version may become effective upon publication through the Company's designated communication channels unless otherwise specified.

The Account Holder is responsible for periodically reviewing the Policy and remaining informed of applicable amendments.

SECTION VI.II: RELATIONSHIP WITH OTHER GOVERNING DOCUMENTS

This Policy shall be read and interpreted together with the Company's Terms of Use and Governance, Data Governance Policy, Investment Risk Disclosure Policy, and any other applicable policies, agreements, disclosures, or notices issued by the Company.

Nothing in this Policy shall limit or replace any obligation imposed by Applicable Law, regulatory requirements, or other governing documents.



Where a provision of this Policy conflicts with a mandatory legal or regulatory requirement, the applicable legal or regulatory requirement shall prevail to the extent of the conflict.

SECTION VI.III: NON-WAIVER

A failure, delay, or omission by the Company in exercising any right, remedy, power, or authority under this Policy shall not constitute a waiver of that right, remedy, power, or authority.

Any waiver shall be effective only where expressly granted by the Company in writing.

The rights and remedies available under this Policy are cumulative and shall not restrict any other rights or remedies available to the Company under Applicable Law, contractual arrangements, or other applicable policies.