

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

ORVEX CAPITAL LIMITED

Company Number: 17388778

Registered Office: 37th Floor, 1 Canada Square, London, United Kingdom, E14 5AA

Document Version: 1.0

Date of Approval by Directors: 3 September 2026

Next Review Date: 3 September 2027

1. PURPOSE AND SCOPE

ORVEX CAPITAL LIMITED ("ORVEX", the "Company", "we", "us" or "our") is committed to preventing its business, services, financial activities and relationships from being used for money laundering, terrorist financing, fraud, sanctions evasion or other financial crime.

This Anti-Money Laundering and Counter-Terrorist Financing Policy ("AML Policy") establishes the Company's internal framework for identifying, assessing, managing and mitigating financial crime risks.

This Policy applies to:

- directors and officers of ORVEX;
- employees and staff;
- contractors and consultants acting on behalf of the Company;
- third-party service providers and processors where relevant to financial crime risk;
- clients, counterparties, investors and business partners where appropriate;
- transactions and financial activities conducted by or on behalf of ORVEX.

All personnel covered by this Policy are expected to comply with the Company's AML procedures and promptly escalate any suspected financial crime or suspicious activity.

2. LEGAL AND REGULATORY FRAMEWORK

ORVEX operates as a company incorporated in the United Kingdom and maintains its financial crime controls with reference to applicable UK laws, regulations and sanctions requirements.

Depending on the nature and circumstances of the Company's activities, the relevant framework may include:

- The Proceeds of Crime Act 2002 (POCA);
- The Terrorism Act 2000;
- The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, where applicable to the Company's activities;
- The Sanctions and Anti-Money Laundering Act 2018;
- applicable UK financial sanctions regimes administered by HM Treasury's Office of Financial Sanctions Implementation (OFSI);
- applicable UK legislation concerning fraud, proceeds of crime and financial crime;
- applicable data protection and privacy requirements.

ORVEX also takes into account relevant international standards and guidance, including the recommendations and principles developed by the Financial Action Task Force (FATF).

The Company will periodically assess whether changes to its business activities result in additional regulatory or AML obligations.

3. RISK-BASED APPROACH

ORVEX applies a risk-based approach to AML and financial crime prevention.

Risk is assessed using factors including:

Customer and Counterparty Risk

- identity and ownership structure;
- nature and purpose of the business relationship;
- source of funds and, where appropriate, source of wealth;
- beneficial ownership;
- PEP status;
- sanctions exposure;
- adverse media;
- previous suspicious or fraudulent activity.

Transaction and Payment Risk

- transaction value;
- transaction frequency;

- unusual transaction patterns;
- unexpected changes in transaction behaviour;
- payment destination;
- source of funds;
- use of cryptocurrency or virtual assets;
- blockchain wallet risk indicators.

Geographic Risk

Additional consideration may be given to:

- sanctioned jurisdictions;
- jurisdictions identified as presenting increased AML/CTF risk;
- jurisdictions with significant levels of financial crime;
- countries associated with corruption, fraud or weak AML controls.

Higher-risk relationships or transactions may require Enhanced Due Diligence (EDD), additional documentation, management approval or refusal of the transaction.

4. DESIGNATED MONEY LAUNDERING REPORTING OFFICER (MLRO)

ORVEX appoints a designated Money Laundering Reporting Officer ("MLRO") responsible for overseeing the Company's AML framework.

MLRO: Kolosovs Artis

Position: Director

The MLRO is responsible for:

- overseeing implementation of this AML Policy;
- maintaining and reviewing AML procedures;
- assessing escalated suspicious activity;
- coordinating internal investigations;
- determining whether a suspicious activity report should be submitted to the relevant authority;
- maintaining appropriate AML records;
- coordinating AML training;
- monitoring changes in applicable AML and sanctions requirements.

Where the MLRO identifies a potential criminal or regulatory matter, the MLRO will determine the appropriate escalation and reporting procedure.

5. CUSTOMER DUE DILIGENCE (CDD)

ORVEX conducts Customer Due Diligence where appropriate before establishing or continuing a business relationship or processing a material transaction.

CDD may include:

Individuals

- full legal name;
- date of birth;
- nationality;
- residential address;
- government-issued identification;
- identity verification;
- purpose and expected nature of the relationship.

Companies and Legal Entities

- legal name;
- company registration number;
- jurisdiction of incorporation;
- registered office;
- incorporation documents;
- directors;
- authorized representatives;
- ultimate beneficial owners;
- ownership percentages;
- nature and purpose of the business relationship.

The Company may request additional information where the information supplied is incomplete, inconsistent or insufficient to establish the identity or risk profile of the relevant party.

6. ENHANCED DUE DILIGENCE (EDD)

Enhanced Due Diligence will be considered where a customer, counterparty or transaction presents an elevated level of risk.

EDD triggers may include:

- high-value transactions;
- cryptocurrency or virtual asset payments;
- transactions involving blockchain wallets with elevated risk indicators;
- exposure to high-risk jurisdictions;
- sanctions concerns;

- PEP status;
- complex or opaque ownership structures;
- unexplained source of funds or wealth;
- adverse media;
- unusual transaction patterns;
- suspected fraud or financial crime;
- transactions inconsistent with the known purpose of the relationship.

EDD may include:

- additional identity verification;
- verification of UBO information;
- source-of-funds checks;
- source-of-wealth checks;
- additional sanctions screening;
- adverse media screening;
- blockchain wallet analysis;
- additional transaction documentation;
- management or MLRO approval before proceeding.

Where risks cannot be adequately mitigated, ORVEX may decline or terminate the relevant relationship or transaction.

7. SANCTIONS AND PEP SCREENING

ORVEX will take reasonable measures to identify potential sanctions exposure.

Relevant individuals and entities may be screened against applicable sanctions and restricted-party lists, including UK sanctions lists and other relevant international sanctions lists where appropriate.

Potential sanctions matches will be reviewed before a transaction is completed.

ORVEX also considers whether customers, counterparties or relevant beneficial owners are Politically Exposed Persons (PEPs), their family members or known close associates.

Where a PEP relationship is identified, enhanced due diligence may be applied, including obtaining additional information concerning source of wealth and source of funds.

8. TRANSACTION AND WALLET SCREENING

Where cryptocurrency or blockchain transactions are involved, ORVEX may conduct wallet and transaction screening before transferring or receiving funds.

Blockchain analytics tools may be used to assess wallet addresses and transaction histories.

Screening may identify exposure to:

- sanctioned entities or addresses;
- stolen funds;
- ransomware;
- darknet-related activity;
- fraud and scams;
- illicit services;
- mixers or tumblers;
- high-risk services;
- other known or suspected criminal activity.

Wallet risk scores and relevant blockchain intelligence may be considered when determining whether a transaction can proceed.

Where a wallet presents an unacceptable or unexplained level of risk, ORVEX may:

1. place the transaction on hold;
2. request additional information;
3. conduct Enhanced Due Diligence;
4. escalate the matter to the MLRO;
5. refuse or cancel the transaction where appropriate.

9. SOURCE OF FUNDS AND SOURCE OF WEALTH

Where required by the Company's risk assessment, ORVEX may request information regarding the source of funds or source of wealth.

Supporting documentation may include:

- bank statements;
- corporate financial records;
- investment agreements;
- transaction records;
- audited financial statements;
- evidence of business activity;
- other reasonable documentation.

The level of verification will be proportionate to the assessed risk.

10. ESCALATION AND SUSPICIOUS ACTIVITY REPORTING

All directors, employees, contractors and relevant representatives are expected to escalate concerns regarding potentially suspicious activity to the MLRO.

Potential indicators include:

- unexplained transactions;
- suspicious cryptocurrency wallets;
- sanctions exposure;
- suspected fraud;
- unexplained source of funds;
- unusual transaction structures;
- transactions involving high-risk jurisdictions;
- attempts to conceal beneficial ownership;
- transactions inconsistent with the stated business purpose.

The MLRO will assess the information and determine whether further investigation, transaction suspension, refusal of the transaction or external reporting is appropriate.

Where legally required, the Company will submit a Suspicious Activity Report (SAR) or other appropriate report to the relevant competent authority, including the UK National Crime Agency (NCA) where applicable.

Personnel must not disclose information concerning a suspicious activity report where such disclosure would breach applicable law or constitute unlawful tipping-off.

11. RECORD KEEPING

ORVEX maintains appropriate records relating to:

- customer and counterparty due diligence;
- UBO verification;
- sanctions and PEP screening;
- risk assessments;
- Enhanced Due Diligence;
- source-of-funds and source-of-wealth checks;
- transaction monitoring;
- blockchain wallet screening;
- suspicious activity investigations;
- internal AML escalations;
- SAR/STR decisions and filings;
- AML training.

AML and CDD records will generally be retained for a minimum of **five years**, or for a longer period where required by applicable law, regulatory requirements, contractual obligations or an ongoing investigation.

Records will be stored securely and access will be restricted to authorized personnel.

12. STAFF TRAINING

ORVEX will provide AML and financial crime training to relevant directors, employees, contractors and personnel whose responsibilities involve financial crime risk.

Training may cover:

- money laundering and terrorist financing risks;
- KYC and KYB procedures;
- customer risk assessment;
- sanctions;
- PEP identification;
- fraud prevention;
- suspicious activity indicators;
- escalation procedures;
- cryptocurrency and blockchain risks;
- wallet screening;
- record keeping;
- confidentiality and tipping-off requirements.

AML training will be provided:

- upon joining the Company where relevant;
- at least annually for personnel with AML-related responsibilities;
- following material changes to AML procedures or applicable requirements;
- where a specific training need is identified.

Training completion may be documented and retained by the Company.

13. THIRD-PARTY SERVICE PROVIDERS

ORVEX may use reputable third-party providers to support its AML and financial crime controls.

Such providers may assist with:

- identity verification;
- company verification;

- sanctions screening;
- PEP screening;
- adverse media screening;
- blockchain analytics;
- wallet screening;
- transaction monitoring;
- fraud detection.

The use of third-party providers does not remove the Company's responsibility for maintaining appropriate financial crime controls.

Where appropriate, third-party providers will be assessed based on their reliability, relevance and suitability for the services provided.

14. DATA PROTECTION AND CONFIDENTIALITY

Information collected as part of AML and CDD procedures will be handled confidentially and in accordance with applicable data protection and privacy requirements.

Personal information will only be accessed, processed, retained and disclosed where there is an appropriate legal, regulatory, contractual or legitimate business basis.

AML investigations and suspicious activity reports will be treated as confidential and disclosed only to authorized persons or competent authorities where legally permitted or required.

15. PROHIBITED AND HIGH-RISK ACTIVITIES

ORVEX will not knowingly facilitate transactions involving:

- proceeds of crime;
- money laundering;
- terrorist financing;
- sanctions evasion;
- fraud;
- stolen funds;
- other unlawful financial activity.

The Company may refuse, suspend or terminate a relationship or transaction where:

- required due diligence cannot be completed;
- the identity or beneficial ownership cannot be satisfactorily established;
- sanctions concerns cannot be resolved;
- source of funds cannot be reasonably established where required;

- significant fraud indicators are identified;
 - blockchain wallet screening identifies unacceptable risk;
 - the overall financial crime risk cannot be adequately mitigated.
-

16. AML GOVERNANCE AND RESPONSIBILITIES

The directors of ORVEX have overall responsibility for ensuring that an appropriate AML framework is maintained.

The MLRO is responsible for day-to-day oversight of AML procedures and escalation of suspicious activity.

Employees and contractors are responsible for:

- following this Policy;
- completing required due diligence;
- identifying and escalating suspicious activity;
- maintaining confidentiality;
- completing required AML training;
- maintaining appropriate records.

Material AML issues will be escalated to the directors and MLRO as appropriate.

17. POLICY REVIEW

This Policy will be reviewed by ORVEX at least **annually** and additionally following any material change to:

- the Company's business activities;
- applicable legislation or regulatory requirements;
- financial crime risks;
- sanctions requirements;
- cryptocurrency or blockchain-related activities;
- internal AML procedures.

The next scheduled review date is **3 September 2027**, unless an earlier review is required.

Any material amendment to this Policy will require approval by the Company's directors.

18. DIRECTORS' APPROVAL

This Anti-Money Laundering and Counter-Terrorist Financing Policy was reviewed and approved by the directors of ORVEX CAPITAL LIMITED on:

3 September 2026

For and on behalf of ORVEX CAPITAL LIMITED

Director Name: Kolosovs Artis

Position: Director

Signature: 

Date: 3 September 2026

Company: ORVEX CAPITAL LIMITED

Company Number: 17388778

Registered Office: 37th Floor, 1 Canada Square, London, United Kingdom, E14 5AA

Policy Version: 1.0

Approval Date: 3 September 2026

Next Review: 3 September 2027