ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

Version 1.0 · September 2026

Veltonmarkets Global LTD. is an International Business Company incorporated in Saint Lucia under the International Business Companies Act, Cap. 12.14, company number 2026-00672. Registered office: Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia.

1. Purpose and scope

1.1 This Anti-Money Laundering and Counter-Terrorist Financing Policy (the "Policy") sets out the framework by which Veltonmarkets Global LTD. (the "Company", "Veltonmarkets", "we" or "us") identifies its clients, monitors their activity, and prevents its services from being used to launder the proceeds of crime or to finance terrorism.

1.2 The Policy applies to every director, officer, employee, contractor and introducing partner of the Company, and to every client relationship, transaction and payment method the Company offers, without exception and regardless of the value involved.

1.3 Money laundering and terrorist financing are serious criminal offences. The Company has no commercial interest that outweighs its obligation to prevent them. Where this Policy conflicts with a commercial objective, this Policy prevails.

1.4 The Company operates a risk-based approach. The measures applied to a given client are proportionate to the money laundering and terrorist financing risk that client presents, assessed on the factors set out in section 5.

2. Legal and regulatory framework

2.1 The Company is incorporated in Saint Lucia and conducts its affairs in accordance with the Money Laundering (Prevention) Act of Saint Lucia and the Anti-Terrorism Act of Saint Lucia, each as amended, together with guidance issued by the Financial Intelligence Authority of Saint Lucia (the "FIA").

2.2 The Company additionally takes account of the recommendations of the Financial Action Task Force (FATF), which represent the international standard for combating money laundering, terrorist financing and the financing of proliferation, and of the sanctions regimes described in section 11.

2.3 Where the Company accepts a client resident in another jurisdiction, it has regard to any additional obligations arising under the law of that jurisdiction, and may decline the relationship where those obligations cannot be met.

3. Definitions

3.1 **Money laundering** is the process by which the proceeds of criminal conduct are converted, transferred, concealed or disguised so as to appear to have a legitimate origin, or by which a person acquires, uses or possesses property knowing or suspecting it to represent such proceeds. It is commonly described in three stages: placement of criminal funds into the financial system, layering through a series of transactions to obscure their origin, and integration into the economy as apparently legitimate wealth.

3.2 **Terrorist financing** is the provision or collection of funds, from any source and whether lawful or unlawful in origin, with the intention or knowledge that they are to be used to carry out an act of terrorism or by a terrorist organisation. Unlike money laundering, the funds concerned need not be the proceeds of crime, and the sums involved are often small.

3.3 **Beneficial owner** means the natural person who ultimately owns or controls a client, or on whose behalf a transaction is conducted. For a corporate client, it includes any natural person holding, directly or indirectly, twenty-five per cent or more of the shares or voting rights, and any person who otherwise exercises control over the management of that entity.

3.4 **Politically exposed person (PEP)** means an individual who is or has been entrusted with a prominent public function, whether domestically, in a foreign country or by an international organisation, together with that person's immediate family members and known close associates. A prominent public function includes a head of state or government, a senior politician, a senior government, judicial or military official, a senior executive of a state-owned enterprise, and an important political party official.

3.5 **Customer due diligence (CDD)** means the measures set out in section 6 by which the Company identifies a client, verifies that identity from reliable and independent sources, understands the purpose of the relationship and the source of the funds employed in it, and monitors the relationship for consistency with that understanding.

4. Governance and responsibility

The Board

4.1 The Board of Directors owns this Policy. It approves the Policy and any amendment to it, appoints the Money Laundering Reporting Officer, allocates the resources necessary for the AML/CFT programme to function, and receives reporting on its operation at least annually.

The Money Laundering Reporting Officer

4.2 The Company appoints a Money Laundering Reporting Officer (the "MLRO") of sufficient seniority, experience and independence to discharge the role. The MLRO reports directly to the Board and has unrestricted access to all client files, transaction records and systems.

4.3 The MLRO is responsible for:

- receiving and assessing internal suspicion reports, and deciding whether a report is to be made to the FIA;
- making disclosures to the FIA and acting as the Company's point of contact with it and with law enforcement;
- maintaining the Company's business-wide risk assessment and reviewing it at least annually;
- approving the establishment or continuation of higher-risk relationships, including those involving PEPs;
- overseeing the screening, monitoring and record-keeping arrangements described in this Policy;
- arranging staff training and verifying that it has been completed;
- reporting to the Board on the operation and effectiveness of the AML/CFT programme.

4.4 A Deputy MLRO is appointed to act in the MLRO's absence with the same authority. The identity and contact details of the MLRO and Deputy are notified to all staff and are kept current.

Employees

4.5 Every employee is responsible for applying this Policy in their own work and for reporting any knowledge or suspicion of money laundering or terrorist financing to the MLRO promptly and without exception. An employee who fails to do so may commit a criminal offence in their own right and will be subject to disciplinary action by the Company.

5. Risk-based approach

5.1 The Company maintains a documented business-wide risk assessment identifying the money laundering and terrorist financing risks to which its business is exposed, having regard to its clients, the jurisdictions in which they reside, its products, its delivery channels and its payment methods. The assessment is reviewed at least annually and whenever a material change occurs in the business.

5.2 Each client is assigned a risk rating of low, medium or high at onboarding, which is reviewed on the triggers set out in clause 5.4. The rating determines the depth of due diligence applied, the frequency of review, and the level of authority required to approve the relationship.

5.3 The following factors, among others, indicate higher risk:

Category	Higher-risk indicators
Client	A politically exposed person, family member or close associate; a client unwilling or unable to provide the documents requested; a client whose stated occupation or income is inconsistent with the sums deposited; a client acting, or appearing to act, on behalf of another person.
Geography	Residence or nationality in a jurisdiction subject to sanctions; a jurisdiction identified by FATF as high-risk or under increased monitoring; a jurisdiction with recognised weaknesses in AML controls, significant corruption, or known terrorist activity.
Structure	A corporate client with an opaque ownership chain, bearer shares, or nominee arrangements without adequate explanation; a trust or foundation whose beneficiaries cannot readily be identified.
Behaviour	Deposits substantially exceeding what the client has disclosed; funding followed by withdrawal with minimal trading; frequent changes of payment instrument or beneficiary; reluctance to explain the source of funds.

5.4 A client's risk rating is reviewed when the client becomes a PEP, changes residence to a higher-risk jurisdiction, materially changes their pattern of activity, is the subject of an internal suspicion report, or at the periodic interval set out in clause 8.4, whichever occurs first.

6. Customer due diligence

6.1 The Company does not accept anonymous accounts, accounts in fictitious names, or numbered accounts. No client may deposit funds or place a trade until the applicable due diligence has been completed and the account approved.

Individual clients

6.2 For an individual, the Company obtains and verifies: full legal name; date of birth; residential address; nationality; and contact details. Verification is by means of:

- **Proof of identity** — a clear, valid, government-issued photographic document showing the full name, date of birth, document number and expiry date. Accepted documents are a passport, national identity card, or driving licence where it carries a photograph.
- **Proof of residence** — a document dated within the preceding three months showing the client's name and residential address, such as a utility bill, bank or card statement, tax assessment, or a letter from a government authority. A document showing only a post office box is not accepted.

6.3 The Company may additionally require a photograph of the client holding the identity document, a short video verification, or a certified copy of a document, where the risk rating or the quality of the material submitted makes it necessary.

Corporate clients

6.4 For a body corporate, the Company obtains and verifies: the certificate of incorporation; the memorandum and articles of association or equivalent constitutional documents; a certificate of good standing where the entity has been in existence for more than twelve months; the registered and trading addresses; the register of directors and of members; evidence of the authority of the person acting for the entity; and full individual due diligence on each director, each authorised trader, and each beneficial owner identified under clause 3.3.

Purpose and source of funds

6.5 The Company establishes the intended purpose and nature of every relationship, and the source of the funds the client will employ. Where a client's deposits exceed the thresholds set by the Company from time to time, or where the risk rating requires it, the Company obtains documentary evidence of the source of funds and, where appropriate, of the client's source of wealth. Acceptable evidence includes payslips, employment contracts, audited accounts, tax returns, evidence of sale of an asset, inheritance documents or investment statements.

Timing

6.6 Due diligence is completed before the business relationship is established. Where verification cannot be completed, the Company does not open the account; where it cannot be completed for an existing client, the Company suspends the account, permits no further deposits or trading, and considers whether a suspicion report is required. Funds already held are returned only to their verified source, and only where doing so would not prejudice an investigation.

7. Enhanced and simplified due diligence

7.1 Enhanced due diligence is applied to every client rated high risk, to every PEP, to any client resident in a jurisdiction identified by FATF as high-risk or subject to increased monitoring, and to any relationship the MLRO considers to warrant it. Enhanced due diligence comprises:

- approval of the relationship by the MLRO before it is established, and approval to continue it thereafter;
- documentary establishment of the source of funds and source of wealth;
- additional verification of identity from a second independent source;
- closer and more frequent monitoring of transactions, with a lower threshold for escalation;
- review of the relationship at least every six months.

7.2 A client who becomes a PEP during the relationship is treated as a PEP from the date the Company becomes aware, and the relationship requires the MLRO's approval to continue.

7.3 Simplified due diligence is not applied by default. Where the Company applies it, it does so only to a demonstrably low-risk category of client, documents the basis for that assessment, and continues to conduct monitoring sufficient to detect unusual activity.

8. Ongoing monitoring

8.1 The Company monitors the activity of every client for the duration of the relationship, to satisfy itself that the transactions conducted remain consistent with its knowledge of the client, their business and their risk profile.

8.2 Monitoring is conducted by a combination of automated rules applied to deposits, withdrawals and trading activity, and human review by trained staff. Automated alerts are reviewed promptly and their disposal is recorded.

8.3 The following, among others, are treated as indicators warranting review:

- deposits inconsistent with the client's declared income, occupation or net worth;
- funds deposited and then withdrawn with little or no intervening trading;
- a series of deposits structured so that each falls below a verification or reporting threshold;
- a withdrawal requested to an account, card or wallet other than the one funded from;
- trading between two accounts that consistently transfers value in one direction;
- use of payment instruments in the name of a third party;
- a client's reluctance to provide information routinely requested, or the provision of information that proves false;
- activity from an IP address or device inconsistent with the client's declared residence, particularly where that address is in a restricted jurisdiction;
- any transaction with no apparent economic or lawful purpose.

8.4 Client records are refreshed periodically: annually for high-risk clients, every two years for medium risk, and every three years for low risk, or sooner where a trigger in clause 5.4 occurs. Expired identity documents are replaced as a condition of continued trading.

9. Payments and funding

9.1 The Company operates the following funding rules, which exist to prevent the transfer of value between unconnected persons through a trading account:

- **Same-name principle** — funds are accepted only from a payment instrument held in the client's own verified name. Third-party payments are rejected and returned to source.
- **Return to source** — withdrawals are paid to the same instrument from which the corresponding deposit was made, up to the amount deposited, before any alternative method is considered.
- **Profit withdrawal** — amounts exceeding the sums deposited are paid by bank transfer to an account in the client's own name, verified before payment.
- **Minimal-trading refunds** — where a client seeks to withdraw funds that have not been exposed to market risk, the Company may return those funds to source only, and considers whether the pattern requires a suspicion report.

9.2 Cash is not accepted in any form and under any circumstances.

9.3 Where the Company accepts funding in virtual assets, it applies additional controls proportionate to the risk, including blockchain analytics to assess the provenance of the funds, and declines transfers connected to sanctioned addresses, darknet marketplaces, mixing services or known fraud.

9.4 A client may hold only the number of accounts the Company permits, and may not open accounts through another person. Accounts identified as being operated by a person other than the account holder are suspended pending investigation.

10. Prohibited and restricted clients

10.1 The Company does not establish or maintain a relationship with:

- a person who cannot or will not satisfy the due diligence requirements of this Policy;
- a person, entity or vessel designated under any sanctions regime listed in section 11, or owned or controlled by such a person;
- a shell bank, or any institution that maintains a correspondent relationship with a shell bank;

- a person reasonably believed to be acting for an undisclosed principal;
- a person under the age of eighteen;
- a resident of a jurisdiction in which the Company does not offer its services, as published on the Company's website and updated from time to time.

10.2 The Company screens for residence in a restricted jurisdiction at registration, at deposit, and periodically thereafter, and may require evidence of residence at any time. An account found to be held by a resident of a restricted jurisdiction is closed and the balance returned to source.

11. Sanctions

11.1 The Company screens every client, beneficial owner, director and authorised representative against the consolidated sanctions lists of the United Nations Security Council, the Office of Foreign Assets Control of the United States Department of the Treasury, the European Union, and His Majesty's Treasury of the United Kingdom, together with any list applicable under the law of Saint Lucia.

11.2 Screening is performed before the relationship is established, on every list update, and at intervals appropriate to the client's risk rating. Screening extends to PEP and adverse media databases.

11.3 A positive match is escalated to the MLRO immediately. Pending resolution, the account is frozen: no deposit, withdrawal, transfer or trade is permitted. Where a match is confirmed, the Company freezes the assets concerned, makes the disclosures required by law, and does not inform the client of the reason.

11.4 The Company does not facilitate any transaction that would breach a sanctions regime, irrespective of where the client is resident or where the transaction is executed.

12. Reporting suspicious activity

12.1 An employee who knows or suspects, or has reasonable grounds to know or suspect, that a client or transaction is connected with money laundering or terrorist financing must report the matter to the MLRO immediately using the Company's internal report form. Suspicion is a lower threshold than proof; an employee must not wait for certainty and must not conduct their own investigation.

12.2 The MLRO considers each internal report, records the decision and the reasons for it, and where the suspicion is not dispelled makes a suspicious transaction report to the FIA within the period prescribed by law. The decision not to report is documented to the same standard as the decision to report.

12.3 **Tipping off.** No person may disclose to a client, or to any third party, that an internal report has been made, that a report has been made to the FIA, or that an investigation is contemplated or under way, where that disclosure is likely to prejudice the investigation. Tipping off is a criminal offence. An enquiry from a client about a frozen account is answered only in terms approved by the MLRO.

12.4 An employee making a report in good faith is protected. The Company will not permit any detriment to an employee by reason of a report having been made, and treats the identity of the reporting employee as confidential.

12.5 Where a report has been made, the Company does not proceed with the transaction concerned without the consent of the FIA where such consent is required, and follows any direction given to it by the FIA or by law enforcement.

13. Record keeping

13.1 The Company retains the following records for a minimum of seven years:

Record	Retention period begins
Identification and verification material, and the risk assessment of the client	On the date the relationship ends
Transaction records, including deposits, withdrawals, transfers and trades	On the date of the transaction
Internal suspicion reports, the MLRO's assessment, and any report to the FIA	On the date of the report
Screening results, alert dispositions and periodic review records	On the date the record was created
Training records and the business-wide risk assessment	On the date the record was created

13.2 Records are kept in a form that permits their reconstruction and their production to a competent authority promptly on request. They are stored securely, are accessible only to those who require them, and are protected in accordance with the Company's data protection obligations. Where a record is the subject of an investigation, it is retained until the Company is informed that it may be destroyed.

14. Training

14.1 Every employee receives AML/CFT training on appointment and at least annually thereafter, with additional training whenever the law, this Policy or the Company's systems change materially.

14.2 Training covers the law and the offences it creates, this Policy, the recognition of the indicators in clauses 5.3 and 8.3, the internal reporting procedure, the prohibition on tipping off, and the consequences for the employee personally of failing to comply.

14.3 Training is tailored to the role: staff in client onboarding, payments, dealing and support receive instruction specific to the risks arising in their work. Attendance and comprehension are recorded and retained under clause 13.1.

15. Independent review

15.1 The adequacy and effectiveness of the AML/CFT programme are reviewed independently of the staff who operate it, at least annually. The review tests whether the controls described in this Policy are applied in practice, and samples client files, alerts and reporting decisions.

15.2 Findings are reported to the Board with recommendations and a remediation timetable. The MLRO reports progress against that timetable until each finding is closed.

16. Outsourcing and reliance on third parties

16.1 The Company may use third parties to perform elements of identification and verification, including electronic verification providers, screening vendors and payment service providers. Responsibility for compliance with this Policy remains with the Company in every case.

16.2 A third party is assessed before engagement and monitored thereafter. The Company obtains the underlying verification material rather than relying on a confirmation alone, and retains it under section 13.

16.3 Introducing partners and affiliates are subject to due diligence, are contractually bound to this Policy, and have their introduced business monitored. An arrangement is terminated where the partner is found to have circumvented these requirements.

17. Consequences of non-compliance

17.1 Failure to comply with this Policy exposes the Company to criminal and civil liability and the individual concerned to prosecution. An employee who fails to comply is subject to disciplinary action up to and including summary dismissal, and the Company will report conduct to the authorities where the law requires it.

17.2 The Company may, without notice and without liability, suspend an account, refuse a transaction, freeze a balance, or terminate a relationship where it considers it necessary to comply with this Policy or with the law.

18. Review of this Policy

18.1 This Policy is reviewed by the MLRO at least annually, and whenever the law, the Company's services, or the risks it faces change materially. Amendments take effect on approval by the Board.

18.2 The current version of this Policy is published on the Company's website. The Company may amend it at any time without prior notice, and the published version prevails.

19. Contact

19.1 Enquiries concerning this Policy, and correspondence for the attention of the Money Laundering Reporting Officer, may be addressed to compliance@veltonmarkets.com or to the registered office of the Company at Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia.

Version 1.0 · Approved September 2026 · Next scheduled review September 2027