MILTRADERS

MILTRADERS L.L.C-FZ

Meydan Free Zone, Dubai, U.A.E.

ANTI-MONEY LAUNDERING & COUNTER-TERRORISM FINANCING POLICY

(AML / CTF Policy)

Version 1.0 · Effective Date: 29 April 2026

Next Review: 29 April 2027

Approved by: Cyril Bernard Odone Martini, Director

Document Control

Field	Value	Notes
Document Title	AML/CTF Policy	Version 1.0
Owner	AML Compliance Officer	Cyril B. O. Martini
Effective Date	29 April 2026	Initial release
Review Frequency	Annual	Or upon material change
Next Review	29 April 2027	—
Distribution	Public	Published on miltraders.com

1. Purpose

MILTRADERS L.L.C-FZ ("MILTRADERS", "the Company", "we", "us") is committed to the highest standards of Anti-Money Laundering ("AML") and Counter-Terrorism Financing ("CTF") compliance. The purpose of this Policy is to ensure that the Company, its directors, employees, contractors and agents fully comply with applicable AML/CTF laws and international best practices, and that the Company is not used, directly or indirectly, as a vehicle for money laundering, terrorism financing, sanctions evasion, or any other financial crime.

This Policy establishes the framework, controls, processes and responsibilities required to detect, prevent and report any suspicious activity arising from the Company's business relationships and transactions.

2. Scope

This Policy applies to:

- All directors, managers, employees, contractors, interns, and agents of MILTRADERS;
- All clients ("Traders") onboarded through any product offered by the Company, including evaluation challenges, professional accounts and instant funded accounts;
- All business relationships, payment flows, and counterparties (payment service providers, banks, technology vendors, affiliates and partners);
- All jurisdictions in which the Company operates, with particular reference to the United Arab Emirates, the European Union, the United Kingdom and the United States.

3. Regulatory Framework

This Policy is designed to comply with, and is informed by, the following primary instruments:

- UAE Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations, and its Implementing Regulation Cabinet Decision No. (10) of 2019, as amended;
- UAE Cabinet Decision No. (74) of 2020 concerning the UAE List of Terrorists and the Implementation of UN Security Council Resolutions;
- Guidelines issued by the UAE Financial Intelligence Unit ("FIU") and the Executive Office for Anti-Money Laundering and Counter-Terrorism Financing;
- Meydan Free Zone regulations and any rules issued by the Free Zone authority concerning licensed entities;
- Recommendations of the Financial Action Task Force ("FATF") and applicable FATF Mutual Evaluation outcomes;

- Sanctions regimes administered by the United Nations Security Council ("UNSC"), the Office of Foreign Assets Control ("OFAC"), the European Union ("EU"), and His Majesty's Treasury ("HMT, UK").

4. Definitions

For the purposes of this Policy:

- **"Money Laundering"** means the process by which the proceeds of crime are converted into ostensibly legitimate assets, including placement, layering and integration.
- **"Terrorism Financing"** means the provision or collection of funds, by any means, with the intention or knowledge that they will be used to carry out terrorist acts.
- **"Beneficial Owner"** means the natural person who ultimately owns or controls a customer, directly or indirectly, holding 25% or more of the shares or voting rights, or otherwise exercising effective control.
- **"PEP" (Politically Exposed Person)** means a natural person who is or has been entrusted with prominent public functions, including their immediate family members and close associates.
- **"CDD" (Customer Due Diligence)** means the process of identifying and verifying the customer's identity, the nature of the relationship, and ongoing monitoring.
- **"EDD" (Enhanced Due Diligence)** means additional due diligence applied to higher-risk customers, including PEPs and customers from high-risk jurisdictions.
- **"SAR" (Suspicious Activity Report)** means a report filed with the UAE FIU through the goAML system in respect of any transaction or attempted transaction giving rise to suspicion.

5. Governance and AML Compliance Officer

The Director of MILTRADERS L.L.C-FZ assumes ultimate responsibility for the implementation, oversight, and effectiveness of this Policy.

The Company designates an **AML Compliance Officer ("AMLCO")** who is responsible for:

1. Implementing and maintaining this Policy and supporting procedures;
2. Conducting and approving Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD");
3. Performing ongoing transaction monitoring and sanctions screening;
4. Filing Suspicious Activity Reports ("SAR") with the UAE FIU through the goAML platform;
5. Acting as the primary point of contact with regulators and competent authorities;

6. Delivering AML/CTF training to all staff at least annually;
7. Maintaining all AML/CTF records in accordance with Section 13 below;
8. Reporting at least annually to the Director on the effectiveness of the AML/CTF programme.

The AMLCO has direct and unrestricted access to all books, records, systems and personnel of MILTRADERS as required to discharge their duties.

6. Risk-Based Approach

MILTRADERS adopts a documented risk-based approach ("RBA") to AML/CTF, allocating compliance resources commensurate with the level of risk presented by each customer, product, delivery channel and jurisdiction.

The Company maintains an AML/CTF Risk Assessment, reviewed at least annually, that considers:

- Customer risk factors (e.g. occupation, source of funds, residency, structure);
- Geographic risk factors (e.g. jurisdictions on FATF grey/black lists, jurisdictions subject to comprehensive sanctions, jurisdictions with weak AML regimes);
- Product and service risk factors (evaluation challenges, professional accounts, instant funded accounts, payouts in fiat or cryptocurrency where offered);
- Delivery channel risk factors (online onboarding, third-party introducers).

7. Customer Due Diligence (CDD)

MILTRADERS applies CDD measures at the establishment of every business relationship, prior to executing any payment or payout, and in any case where there are doubts about previously obtained customer information.

7.1 Identification and Verification

Each individual Trader must provide and have verified:

- Full legal name as per government-issued identification;
- Date of birth, nationality and country of residence;
- Government-issued photo identification (passport or national ID with machine-readable zone);
- Proof of residential address dated within the last three (3) months (utility bill, bank statement, government letter);
- Email address and phone number, both verified through one-time codes;
- Source of funds declaration where applicable.

Verification is performed using a combination of automated identity verification tools (including liveness check and document authenticity checks), database screening, and human review by the AMLCO.

7.2 Corporate Customers

Where a Trader is a legal entity, additional documentation is required, including but not limited to: certificate of incorporation, register of directors, register of shareholders, beneficial ownership declaration identifying any natural person holding 25% or more, and a board resolution authorising the relationship.

7.3 Ongoing Monitoring

CDD is not a one-off exercise. Customer files are reviewed periodically based on risk rating: low-risk every 36 months, medium-risk every 24 months, high-risk every 12 months, and immediately upon any trigger event (change of country, unusual transaction, sanctions hit, adverse media).

8. Enhanced Due Diligence (EDD)

EDD is mandatory and must be approved by the AMLCO before establishing or continuing the relationship in any of the following situations:

- The customer is a PEP, family member of a PEP, or known close associate of a PEP;
- The customer is established or resident in a jurisdiction identified by the FATF as having strategic deficiencies, or in a jurisdiction subject to comprehensive UAE, UN, OFAC, EU or HMT sanctions;
- The customer presents an unusually complex ownership or control structure;
- There are indications of adverse media regarding the customer or any of its controllers;
- The customer requests anonymity, refuses to provide standard documentation, or attempts to circumvent normal procedures.

EDD measures include obtaining additional documentation on source of funds and source of wealth, obtaining senior management approval (Director sign-off), increased frequency of file reviews, and enhanced ongoing transaction monitoring.

9. Politically Exposed Persons (PEPs)

All customers are screened against PEP databases at onboarding and on an ongoing basis (daily delta screening). When a positive match is confirmed, the relationship is escalated to the AMLCO and may be onboarded only with EDD and Director approval. Family members and known close associates of PEPs are treated as PEPs.

10. Sanctions Screening

MILTRADERS does not establish or maintain business relationships with, and does not process any transaction involving, any natural or legal person, vessel, aircraft or jurisdiction that is the target of UN, UAE, OFAC, EU or HMT sanctions.

All customers, beneficial owners, and counterparty payment instruments are screened at onboarding and on an ongoing basis against:

- UAE Local Terrorist List and UN Consolidated Sanctions List;
- OFAC SDN List and Sectoral Sanctions Identifications List;
- EU Consolidated List of Persons, Groups and Entities subject to EU Financial Sanctions;
- UK HMT Consolidated List of Financial Sanctions Targets.

In the event of a confirmed match, the assets of the relevant person shall be frozen without delay, no further transaction shall be executed, and a report shall be filed with the UAE FIU and any other competent authority within the timeframes prescribed by law.

11. Transaction Monitoring

Customer transactions, including initial fee payments, addon purchases and payouts, are subject to automated and manual monitoring designed to detect:

- Inconsistency between the transaction profile and the customer's declared profile;
- Use of multiple accounts or aliases by the same individual;
- Structuring or smurfing patterns (multiple small transactions designed to avoid thresholds);
- Payments to or from high-risk or sanctioned jurisdictions;
- Payments via instruments not held in the customer's name;
- Sudden change in trading style or volume that is inconsistent with skill development.

Alerts generated by monitoring rules are reviewed by the AMLCO. Customer relationships that present a confirmed material concern shall be terminated and reported as required.

12. Suspicious Activity Reporting (SAR)

Where the AMLCO has reasonable grounds to suspect that any transaction, attempted transaction, or property is connected to money laundering, terrorism financing, or any predicate offence, a Suspicious Activity Report shall be filed with the UAE Financial Intelligence Unit through the goAML system without delay.

Filing of a SAR is mandatory regardless of the amount involved, the customer's status, and whether the transaction is ultimately completed. The fact that a SAR has been filed, the

contents of the SAR, and any communication with the FIU are strictly confidential and shall not be disclosed to the customer or to any third party (no tipping-off).

13. Record Keeping

MILTRADERS retains all AML/CTF-related records, including identification documents, due diligence records, transaction records, internal reports, SARs and supporting analysis, for a minimum period of five (5) years from the end of the business relationship or the date of the transaction, whichever is later, in accordance with UAE Federal Decree-Law No. (20) of 2018.

Records are stored securely in encrypted form, with access restricted to authorised personnel on a need-to-know basis, and are made available to the UAE FIU and competent authorities upon lawful request.

14. Training and Awareness

All employees, contractors, and agents involved in onboarding, customer support, payments or compliance receive AML/CTF training upon hire and at least annually thereafter. Training covers, at a minimum: the legal framework, red flags, the Company's internal procedures, the SAR escalation process, and the prohibition on tipping-off. Training attendance and outcomes are documented and retained.

15. Internal Controls and Independent Review

The AMLCO performs an annual self-assessment of the AML/CTF programme. In addition, the Company commissions, no less frequently than every two (2) years, an independent review of the effectiveness of this Policy and its implementation. The findings are reported to the Director and remediation actions tracked to closure.

16. Whistleblowing and Non-Retaliation

Any director, employee, contractor, or third party who suspects a breach of this Policy or any AML/CTF law may report it confidentially to the AMLCO. The Company strictly prohibits any form of retaliation against any person making a good-faith report.

17. Sanctions for Non-Compliance

Failure by any director, employee or contractor to comply with this Policy may result in disciplinary action up to and including termination, and may also result in personal civil and/or criminal liability under applicable laws.

18. Policy Review and Updates

This Policy is reviewed at least annually and following any material change in regulation, business model, or risk profile. The current version is published on the Company's website at miltraders.com/aml-policy and made available to all stakeholders.

19. Contact

Any question concerning this Policy, or any matter relating to AML/CTF compliance, should be directed to the AML Compliance Officer:

- AML Compliance Officer: Cyril Bernard Odone Martini, Director
- Email: compliance@miltraders.com
- Postal address: MILTRADERS L.L.C-FZ, Meydan Grandstand, 6th Floor, Meydan Road, Nad Al Sheba, Dubai, U.A.E.

— END OF POLICY —

Approved and signed for and on behalf of MILTRADERS L.L.C-FZ:

Cyril Martini

Cyril Bernard Odone Martini
Director & AML Compliance Officer
Date: 29 April 2026