Mento MARKETS

AML/CFT Policy

CONTENT

1. Purpose and Policy Statement
2. Scope
3. Regulatory and Standards Framework
4. Business and Risk Profile
5. Governance and Oversight
6. Roles and Responsibilities
7. Risk-Based Approach and Customer Risk Rating
8. Customer Acceptance and Prohibited Relationships
9. Customer Due Diligence
10. KYC Refresh and Periodic Review Frequency
11. Enhanced Due Diligence
12. Politically Exposed Persons, Sanctions, and Screening
13. Client Onboarding Controls for MT5 Operations
14. Ongoing Monitoring and Alert Framework
15. Payments, Funding, and Withdrawal Controls
16. Customer Refusal, Restriction, and Termination Workflow
17. Suspicious Activity Identification and Reporting
18. Sanctions Compliance and Asset Freezing
19. Record Keeping
20. Reliance, Outsourcing, and Third Parties
21. Staff Screening and Training
22. Monitoring, Independent Testing, and Review
23. Data Protection, Confidentiality, and Information Sharing
24. Breaches and Disciplinary Measures
25. Effective Date and Approval
26. Board Approval Block

Mento Markets Ltd.
Ground Floor, the Sotheby Building,
Rodney Village, Rodney Bay, Gros-Islet,
Saint Lucia.

1. Purpose and Policy Statement

This Anti-Money Laundering and Countering the Financing of Terrorism Policy (the Policy) establishes the framework adopted by Mento Merkets Ltd. (the Company) to prevent, detect, and report money laundering, terrorist financing, proliferation financing, sanctions breaches, fraud-related abuse, and other financial crime risks associated with its business. The Policy is designed for a CFD brokerage business providing online trading services, including account opening, funding, trading, and withdrawal activity through MetaTrader 5 (MT5), related websites, client portals, payment channels, and associated support functions.

The Company applies a risk-based approach to AML/CFT compliance, under which customers, products, services, delivery channels, geographies, payment methods, and transactional behaviour are assessed and monitored in a manner proportionate to identified risks. This approach reflects the Saint Lucia Money Laundering (Prevention) Act, record-retention obligations in Saint Lucia law, applicable counter-terrorism and sanctions obligations, and the FATF risk-based approach for the securities sector.

The Company maintains zero tolerance for knowingly facilitating money laundering, terrorist financing, sanctions evasion, market abuse, fraud, identity misuse, third-party funding abuse, or other criminal conduct. All directors, officers, employees, contractors, and relevant agents must comply with this Policy and all related procedures, guidance, and internal controls.

2. Scope

This Policy applies to the entire business of the Company, including:

- Retail and professional client onboarding.
- Individual, joint, and corporate client relationships.
- Introducers, affiliates, white-label partners, payment service providers, technology vendors, and other third parties where applicable.
- All business lines involving CFD trading and ancillary services made available through MT5 or any successor platform.
- All employees, senior management, directors, compliance personnel, and outsourced service providers performing regulated or control functions.

This Policy covers customer due diligence, risk classification, KYC refresh, ongoing monitoring, sanctions and PEP screening, suspicious activity identification, internal escalation, external reporting, employee training, governance, independent testing, record retention, and periodic review.

3. Regulatory and Standards Framework

The Company designs and administers this Policy with reference to the following framework, as applicable to its operations in and from Saint Lucia:

- The Money Laundering (Prevention) Act of Saint Lucia.
- The Proceeds of Crime Act provisions on retention of records by financial institutions, including a seven-year retention period for account opening records after account closure and seven years for other transaction-related records after the transaction date.
- Applicable anti-terrorism and counter-terrorist financing legal obligations in Saint Lucia.
- The United Nations sanctions obligations and related compliance expectations reflected in Saint Lucia compliance notices.
- Guidance and expectations issued by the competent authorities of Saint Lucia, including the Financial Services Regulatory Authority and the Financial Intelligence Authority, where relevant.
- FATF Recommendations and the FATF risk-based approach guidance for the securities sector, including the requirement to keep CDD information up to date through ongoing monitoring and periodic review, especially for higher-risk customers.

Where the Company is subject to additional requirements through correspondent banking, payment providers, technology partners, contractual obligations, or foreign-facing business relationships, the stricter standard may be adopted where appropriate to manage legal and reputational risk.

4. Business and Risk Profile

The Company operates as an online CFD brokerage business using MT5 infrastructure to provide leveraged trading access to eligible clients. The business model presents financial crime risks that differ from traditional retail commerce because clients may be on boarded remotely, fund accounts electronically, trade rapidly across multiple instruments, and request withdrawals through digital channels, all of which require enhanced identity controls and behavioral monitoring.

The Company therefore recognizes, among others, the following inherent risk drivers:

- Non-face-to-face onboarding.
- Cross-border client acquisition.
- Use of leverage and rapid order activity.
- Third-party payment or refund attempts.
- High-volume deposits and withdrawals inconsistent with known profile.
- Dormant accounts becoming suddenly active.
- Potential misuse of trading accounts to layer funds or obscure beneficial ownership.
- Exposure to sanctioned persons, PEPs, adverse media concerns, or high-risk jurisdictions.

5. Governance and Oversight

The Board of Directors bears ultimate responsibility for ensuring that the Company maintains an effective AML/CFT governance framework. The Board shall approve this Policy, approve the Company's AML/CFT risk appetite, review material AML/CFT reports at least annually, provide adequate compliance resources, and ensure that senior management fosters a culture of compliance and escalation.

Senior management is responsible for implementing this Policy in daily operations, ensuring effective procedures, assigning competent personnel, remedying identified weaknesses, and supporting the Money Laundering Reporting Officer (MLRO) and any deputy or alternate compliance officer.

The MLRO shall have appropriate authority, independence, and direct access to senior management. The MLRO is responsible for receiving internal suspicious activity reports, determining whether an external report must be filed with the competent authority, overseeing sanctions and screening controls, maintaining AML/CFT records, coordinating investigations, and ensuring periodic reporting to senior management.

6. Roles and Responsibilities

6.1 Board of Directors

The Board shall:

- Approve the AML/CFT framework and material amendments.
- Ensure regular assessment of the Company's money laundering, terrorist financing, sanctions, and proliferation financing risks.
- Review significant compliance breaches, audit findings, suspicious activity trends, and regulatory issues.
- Ensure the independence and effectiveness of the compliance function.
- Review the results of independent AML/CFT testing at least annually.

6.2 Senior Management

Senior management shall:

- Implement Board-approved AML/CFT controls.
- Allocate sufficient staffing, systems, and training.
- Ensure onboarding, payments, dealing, and customer support teams apply approved procedures.
- Escalate material AML/CFT matters promptly.
- Ensure remediation plans are implemented within agreed deadlines.

6.3 MLRO / Compliance Function

The MLRO and compliance function shall:

- Maintain AML/CFT procedures, risk assessments, and control testing.
- Review higher-risk accounts, alerts, unusual activity, and sanctions matches.
- Receive and assess internal reports of suspicious activity.
- Make timely external filings where required by law.
- Liaise with competent authorities, auditors, and relevant counterparties on AML/CFT matters.
- Oversee training, monitoring, policy review, and periodic rescreening.

6.4 Employees and Relevant Personnel

All employees and relevant personnel shall:

- Comply with this Policy and related procedures.
- Complete mandatory training before handling relevant functions and thereafter on a periodic basis.
- Promptly escalate unusual activity, documentary irregularities, sanctions concerns, or suspected evasion.
- Maintain confidentiality and avoid tipping off any person who is the subject of a review or report.

7. Risk-Based Approach and Customer Risk Rating

The Company shall identify, assess, document, and periodically review money laundering, terrorist financing, sanctions, and proliferation financing risks across the business. The enterprise-wide risk assessment shall consider at least the following categories:

- Customer risk.
- Product and service risk.
- Delivery channel risk.
- Geographic risk.
- Transaction and payment risk.
- Third-party and outsourcing risk.
- Technology and cyber-enabled abuse risk.

Customers shall be assigned a risk rating using a documented scoring methodology. The methodology may be automated or manual, but must be approved by Compliance and reviewed at least annually. The minimum scoring categories shall be as follows:

Risk Factor	Low Indicator	Medium Indicator	High Indicator
Jurisdiction	Resident/incorporated in standard-risk jurisdiction	Cross-border but acceptable jurisdiction	High-risk, sanctioned-adjacent, or otherwise restricted jurisdiction
Customer Type	Natural person with simple profile	Legal entity with straightforward ownership	PEP, complex structure, nominee involvement, or opaque ownership
Delivery Channel	Standard digital onboarding with clean verification	Non-face-to-face with minor exceptions resolved	Non-face-to-face with elevated impersonation or document integrity concerns
Funding Method	Same-name bank/card funding	Mixed but explainable funding routes	Third-party funding, unusual routing, multiple unrelated instruments
Activity Pattern	Consistent with stated profile	Moderately higher-than-expected activity	Rapid deposits/withdrawals, unusual turnover, or behaviour inconsistent with profile
Adverse Information	None	Limited adverse information requiring review	Negative media, law-enforcement nexus, sanctions proximity, or fraud concerns

The customer risk-rating score shall be calibrated on the following basis:

- 0 to 5 points: Low risk.
- 6 to 11 points: Standard risk.
- 12 points or more: High risk.
- Any sanctions match, confirmed false identity, prohibited jurisdiction, unverified beneficial ownership, or unresolved adverse media with serious criminal implications shall override the numeric score and require decline, exit, or senior management escalation.

Customers shall be assigned review and control measures proportionate to their risk level. Risk scoring may take into account residence or incorporation jurisdiction, source of wealth, source of funds, occupation or business activity, expected account usage, payment methods, adverse media, PEP status, sanctions proximity, ownership complexity, use of intermediaries, and behavioral indicators observed after onboarding.

8. Customer Acceptance and Prohibited Relationships

The Company shall establish customer acceptance criteria consistent with its risk appetite. The Company may decline or exit a relationship where the prospective or existing client:

- Fails or refuses to provide required identification or verification information.
- Uses false, altered, inconsistent, or suspicious documentation.
- Seeks to fund or withdraw through unrelated third parties without a legitimate explanation.
- Is located in, resident in, incorporated in, or closely connected to a prohibited or unacceptable jurisdiction under Company policy.
- Appears on an applicable sanctions list or is linked to a sanctioned person or entity.
- Presents unmanageable money laundering, terrorist financing, fraud, chargeback, market abuse, or reputational risk.
- Attempts to circumvent onboarding, screening, or payment controls.

The Company shall not establish or maintain anonymous accounts, fictitious-name accounts, or relationships where beneficial ownership cannot be reasonably identified and verified.

9. Customer Due Diligence

9.1 General Standard

Customer due diligence (CDD) must be completed before establishing a business relationship, activating trading functionality, or processing material account funding, except where delayed completion is expressly permitted by law and risk controlled. CDD must be proportionate to risk and sufficient to identify the customer, understand the purpose and intended nature of the relationship, and support ongoing monitoring.

9.2 Individual Clients

For individuals, the Company shall obtain and verify, at a minimum, information such as:

- Full legal name.

• Date of birth.

• Nationality.

• Residential address.

• Valid government-issued identification number and copy of identification document.

• Contact details.

• Occupation or employment/business information.

• Source of funds and, where appropriate, source of wealth.

• Expected trading activity and payment profile.

The Company may use documentary and non-documentary methods to verify identity and address, including electronic verification, biometric checks, liveness checks, database searches, and consistency checks across onboarding records, payment information, IP data, device signals, and other digital evidence, where legally and operationally appropriate.

9.3 Corporate and Legal Entity Clients

For companies, partnerships, trusts, and other legal arrangements, the Company shall obtain and verify, as applicable:

• Legal name, registration number, registered office, and principal place of business.

• Certificate of incorporation or equivalent constitutional documents.

• Nature of business.

• Identity of directors, authorized signatories, controllers, and beneficial owners.

• Ownership and control structure.

• Board resolution or authority documentation for account opening.

• Source of funds and, where appropriate, source of wealth.

• Expected trading strategy, transactional profile, and funding arrangements.

Where ownership chains are layered or cross-border, the Company shall obtain sufficient documentation to understand the ultimate beneficial ownership and control structure. Enhanced scrutiny shall be applied where nominee arrangements, trusts, bearer-style features, or opaque vehicles are involved.

9.4 Beneficial Ownership

The Company shall identify and verify the natural persons who ultimately own or control a legal entity client, directly or indirectly, or otherwise exercise effective control. Where no individual clearly meets an ownership threshold under applicable law or policy, the Company shall identify the relevant senior managing official or equivalent controlling person and document the rationale.

9.5 Purpose and Intended Nature

The Company shall understand why the customer seeks the relationship and how the account is expected to be used. For a CFD broker, this includes collecting information relevant to intended trading activity, approximate funding levels, expected deposit and withdrawal behaviour, trading knowledge where relevant to onboarding controls, and whether the client acts on its own behalf or through an intermediary.

10. KYC Refresh and Periodic Review Frequency

The Company shall keep CDD and KYC information current through trigger-based reviews and scheduled periodic refresh cycles. Periodic review frequencies shall be aligned to customer risk rating as follows, reflecting the FATF requirement to keep customer information up to date through ongoing monitoring and more frequent review for higher-risk relationships.

Risk Tier	Minimum KYC Refresh Frequency	Trigger Events Requiring Immediate Review
Low Risk	Every 36 months	Material profile change, sanctions/PEP hit, unusual funding or withdrawal pattern
Standard Risk	Every 24 months	Material profile change, adverse media, linked-account concerns, abnormal trading/payment activity
High Risk	Every 12 months	Any material change, heightened monitoring alert, ownership change, source-of-funds concern, sanctions/PEP development
PEP / Sanctions-Adjacent / Exception Cases	Every 6 months or more frequently as directed by MLRO	Any change in status or material activity anomaly

Trigger events shall include expired identification documents, change of address, change of beneficial ownership, payment-instrument change, inactivity followed by sudden reactivation, unexplained increase in funding volume, high-risk jurisdiction nexus, or system-generated concern.

11. Enhanced Due Diligence

Enhanced due diligence (EDD) shall be applied where higher risk is identified, including but not limited to:

- PEPs and their family members or close associates, where applicable.
- Clients from or connected to high-risk or sanctioned jurisdictions.
- Complex or unusual ownership structures.
- Higher-value accounts or significant funding patterns.
- Adverse media or negative intelligence indicators.
- Non-face-to-face onboarding presenting elevated impersonation or identity fraud risk.
- Cases involving unusual payment routing, multiple cards, and virtual assets interfaces, or repeated failed funding attempts.

EDD measures may include obtaining additional identification documents, enhanced source of funds/source of wealth evidence, senior management approval, increased transaction monitoring, more frequent KYC refresh, independent corroboration of ownership and business activity, and restrictions on payment methods or withdrawal routes.

12. Politically Exposed Persons, Sanctions, and Screening

The Company shall screen prospective and existing clients, beneficial owners, authorized persons, counterparties where relevant, and applicable transactions against sanctions lists, terrorist lists, PEP databases, and adverse media sources before onboarding and on an ongoing basis. Saint Lucia compliance notices direct financial institutions and relevant supervised businesses to check applicable United Nations sanctions lists and comply immediately with legal requirements concerning listed persons and entities.

The minimum screening frequency shall be:

- At onboarding, before account approval.

• Daily automated rescreening where systems permit, and in any event not less than weekly batch rescreening of the full customer base.

• Event-driven rescreening upon profile amendments, beneficial ownership changes, payment-method changes, reactivation of dormant accounts, material withdrawals, or relevant legal/regulatory updates.

• Ad hoc rescreening when new sanctions lists, PEP status changes, or adverse media developments are identified.

Potential matches shall be reviewed promptly by compliance personnel using risk-based procedures. True matches or legally significant near matches shall trigger immediate escalation, restriction or freezing action where required, rejection or suspension of the relationship where appropriate, and reporting to the competent authority in accordance with applicable law.

PEP relationships shall be subject to risk-sensitive treatment, including enhanced review, source of wealth/source of funds assessment, senior management approval where required, and intensified ongoing monitoring.

13. Client Onboarding Controls for MT5 Operations

Because the Company provides services through MT5 and associated online channels, onboarding controls shall address risks specific to remote CFD brokerage activity. These controls may include:

• Verification before issuance of full trading access.

• Validation of email, phone number, and digital account credentials.

• Review of IP geolocation, device consistency, and access anomalies.

• Detection of duplicate or linked profiles, including shared identifiers, payment instruments, addresses, devices, or behavioral overlap.

• Restrictions on third-party deposits and withdrawals.

• Review of rapid funding followed by minimal trading and early withdrawal requests.

• Controls over account reactivation, password resets, and profile changes that may indicate account takeover or impersonation.

• Monitoring of introducing broker, affiliate, or referral patterns where these may mask beneficial ownership or control.

The Company may impose pre-trade, funding, or withdrawal restrictions until required due diligence is complete and risk concerns are resolved.

14. Ongoing Monitoring and Alert Framework

The Company shall conduct ongoing monitoring throughout the customer relationship to ensure that documents, information, and risk understanding remain current and that transactions are consistent with the customer's known profile. Ongoing monitoring is a core element of the FATF risk-based approach and is particularly relevant to securities and trading activity where account behaviour can change rapidly.

Monitoring shall be manual, automated, or hybrid, and shall include review of deposits, withdrawals, internal transfers where applicable, changes in trading behaviour, changes in control or beneficial ownership, profile amendments, login anomalies, screening hits, and other indicators of unusual conduct. The extent and frequency of monitoring shall reflect risk.

The Company shall maintain documented alert categories and threshold logic. Unless stricter thresholds are set in procedures or systems, the following minimum alert categories shall apply:

Alert Category	Minimum Trigger
Rapid Funding and Withdrawal	Aggregate deposits and requested withdrawals of USD 10,000 or more within 7 calendar days with limited or no meaningful trading activity
Unusual Deposit Size	Single deposit of USD 10,000 or more inconsistent with stated profile or expected activity
Aggregate Funding Spike	Aggregate deposits of USD 25,000 or more within 30 calendar days for a standard-risk client, absent clear economic rationale
Third-Party Funding Concern	Any attempted deposit or withdrawal involving a name mismatch or unrelated third party
Dormant Account Reactivation	Account inactive for 6 months or more, followed by funding, credential reset, or withdrawal request
Linked Account Behaviour	Shared devices, IPs, payment methods, addresses, or identifiers across multiple accounts without satisfactory explanation
High-Risk Jurisdiction Touchpoint	Any login, funding route, or customer-profile nexus involving a prohibited or high-risk jurisdiction under Company policy

Payment Fragmentation	Five or more failed or split funding attempts within 24 hours
Withdrawal Escalation	Single withdrawal of USD 10,000 or more, or cumulative withdrawals of USD 20,000 or more within 30 days, inconsistent with profile
Adverse Media / Sanctions Update	Any new screening hit or material negative intelligence

Examples of potentially suspicious indicators in a CFD/MT5 environment include:

- Funding followed by little or no genuine trading and a withdrawal request.
- Multiple payment methods or repeated use of cards/accounts not in the client's name.
- Deposit and withdrawal activity inconsistent with stated occupation, income, or source of funds.
- Multiple accounts that appear linked without a valid disclosed reason.
- Trading patterns suggestive of collusion, wash-like behaviour, or use of accounts primarily for value transfer rather than bona fide investment activity.
- Frequent changes to key account details shortly before withdrawals.
- Sudden activity involving clients previously dormant or assessed as low risk.
- Attempts to avoid verification thresholds or provide piecemeal explanations for unusual conduct.

Compliance shall review alerts promptly, document the outcome, escalate unusual cases to the MLRO, and revise thresholds where business volume, product mix, or risk exposure changes materially.

15. Payments, Funding, and Withdrawal Controls

The Company shall maintain controls over account funding and withdrawals proportionate to the risk of misuse. As a general principle, the Company shall seek to ensure that funds are received from, and returned to, an account or payment instrument in the client's own name, subject to lawful exceptions approved under documented procedures.

The Company may restrict, reject, reverse, or hold transactions where:

- The payer or recipient appears unrelated to the client.
- The payment route is opaque or commercially unnecessary.
- The transaction is inconsistent with known customer information.
- There is a sanctions, fraud, chargeback, or suspicious activity concern.
- Additional source of funds evidence is required.

Heightened review shall apply to unusual card usage, e-wallet activity, multiple failed deposits, rapid in-and-out flows, payment fragmentation, repeated refunds, and withdrawal requests following negligible market exposure.

16. Customer Refusal, Restriction, and Termination Workflow

Where CDD or EDD cannot be completed satisfactorily, the Company shall not open the account, shall not activate trading access, and shall not process discretionary withdrawals except where required by law or directed by competent authority. If the relationship already exists, the Company shall consider restricting activity, suspending the account, rejecting further funding, refusing withdrawals to third parties, and terminating the relationship in a controlled manner, subject to legal and reporting requirements.

The minimum workflow shall be:

1. Place the account in pending, restricted, or review status.
2. Request outstanding information or clarification within a defined period set by Compliance.
3. Escalate unresolved or high-risk matters to the MLRO.
4. Determine whether suspicion exists and whether an external report is required.
5. Approve decline, continued restriction, or exit decision through Compliance and, for high-risk cases, senior management.
6. Record the rationale, actions taken, and whether any reporting or freezing obligation applies.

No customer shall be on boarded or retained where identity, beneficial ownership, source of funds, sanctions status, or risk profile cannot be brought within the Company's risk appetite and legal obligations.

17. Suspicious Activity Identification and Reporting

All employees must remain vigilant for facts, behaviors, or circumstances that may indicate money laundering, terrorist financing, sanctions evasion, fraud, or other criminal conduct. Suspicion may arise from a single event or a pattern of behaviour and does not require proof of an underlying offence.

Any employee who knows, suspects, or has reasonable grounds to suspect suspicious activity shall submit an internal report to the MLRO without delay and in the prescribed form or channel. The internal report must contain all relevant facts, supporting records, and a clear explanation of the concern.

Upon receipt of an internal report, the MLRO shall promptly assess the matter, determine whether further internal investigation is warranted, decide whether the matter requires external reporting to the Financial Intelligence Authority or other competent authority, and document the rationale for the decision. External suspicious transaction or suspicious activity reports shall be filed as required by applicable law, and related records shall be retained securely.

No employee shall disclose to the client or any third party that a suspicion has been formed, an internal report has been made, an external report has been filed, or that a law enforcement or regulatory inquiry is contemplated or underway, except as permitted by law. Tipping off and improper disclosure are strictly prohibited.

18. Sanctions Compliance and Asset Freezing

The Company shall maintain sanctions controls reasonably designed to prevent dealings with sanctioned persons, entities, countries, vessels, or other restricted targets, as applicable. Screening shall be undertaken at onboarding, periodically thereafter, on material profile changes, and prior to or during processing of relevant transactions, using risk-based logic and updated lists.

Where an asset freeze, prohibition, or reporting requirement applies, the Company shall act immediately in accordance with applicable law and internal escalation procedures. This may include blocking transactions, freezing accounts or assets, halting withdrawals, preserving evidence, notifying the MLRO and senior management, and making required reports to the competent authority.

19. Record Keeping

The Company shall create and retain complete and retrievable records sufficient to demonstrate compliance with legal and regulatory obligations and to support reconstruction of transactions and investigations. Records shall include, as applicable:

• Customer identification and verification records.

• Beneficial ownership information.

• Risk assessments and customer risk ratings.

• Screening results and resolution of matches.

• Account files, communications, and onboarding approvals.

• Payment, transaction, and trading records.

• Internal suspicious activity reports and related MLRO decisions.

• External reports and regulatory correspondence.

• Training records, audit findings, and policy review records.

The Company shall retain records in accordance with Saint Lucia law as follows:

• Account opening and account relationship records: seven years after the account is closed.

• Other transaction-related records: seven years after the date of the transaction.

• AML/CFT investigation, alert, and suspicious activity records: at least seven years from closure of the matter, and longer where litigation, regulatory inquiry, or investigation is ongoing or reasonably anticipated.

Records shall be stored in original, electronic, microfilm, or other retrievable form that permits timely production to competent authorities, auditors, or other authorized persons.

20. Reliance, Outsourcing, and Third Parties

Where the Company relies on third parties, vendors, affiliates, introducers, payment service providers, or outsourced service providers for elements of onboarding, screening, payments, technology, or monitoring, the Company remains responsible for ensuring that AML/CFT obligations are effectively discharged unless law expressly provides otherwise.

Before entering into or continuing such arrangements, the Company shall conduct appropriate due diligence on the third party, assess legal and operational risk, define responsibilities contractually, ensure access to records and audit rights where appropriate, and monitor performance on an ongoing basis. Higher scrutiny shall apply to parties that can influence client acquisition, client identification, payment routing, or transaction execution.

21. Staff Screening and Training

The Company shall implement appropriate pre-employment and ongoing screening of employees and relevant personnel in accordance with law and proportionality. Employees engaged in onboarding, payments, customer support, dealing, risk, compliance, technology, and management functions shall receive AML/CFT training relevant to their roles.

Training shall be provided on the following minimum cadence:

Role Category	Minimum Training Cadence
All Staff	At induction and annually thereafter
Onboarding, Payments, Support, and Dealing Staff	At induction, annually, and targeted refreshers when typologies or controls change
Compliance, MLRO, and Senior Management	At induction and at least semi-annually, including regulatory update sessions
High-Risk Functions or Remediation Cases	Additional ad hoc training within 30 days of identified deficiency or material incident

Training shall cover at least legal obligations, internal procedures, escalation routes, suspicious activity indicators, sanctions compliance, tipping-off restrictions, data protection considerations, and financial crime risks specific to online CFD and MT5 operations. Training completion shall be documented and non-completion shall be escalated to management.

22. Monitoring, Independent Testing, and Review

The Company shall test the effectiveness of this Policy and its related procedures through compliance reviews, control testing, internal audit where applicable, exception reporting, quality assurance, and remediation tracking. Material weaknesses, overdue actions, and significant incidents shall be reported to senior management and, where appropriate, to the Board.

Independent AML/CFT testing shall be conducted at least annually. Such testing shall be performed by internal audit personnel independent from the day-to-day AML/CFT control owners, or by a suitably qualified external reviewer where internal independence is not available. The scope shall include customer onboarding, risk-rating methodology, KYC refresh compliance, sanctions screening, transaction monitoring, suspicious activity escalation, record retention, and staff training effectiveness.

This Policy shall be reviewed at least annually and sooner where there is a material change in law, regulation, business model, platform functionality, products, geographic exposure, payment methods, customer risk profile, or identified control weakness. Amendments shall be approved through the Company's governance process.

23. Data Protection, Confidentiality, and Information Sharing

The Company shall process personal and business information used for AML/CFT purposes lawfully, securely, and only to the extent necessary for compliance, risk management, fraud prevention, sanctions screening, and related legal obligations. Access to AML/CFT information shall be restricted to authorized personnel with a need to know.

Information may be shared internally or with competent authorities, auditors, legal advisers, banks, payment providers, or other permitted counterparties where required or permitted by law and for legitimate AML/CFT, sanctions, fraud prevention, or investigative purposes. Confidentiality obligations shall not prevent lawful reporting or escalation.

24. Breaches and Disciplinary Measures

Any breach of this Policy, related procedures, or lawful AML/CFT instruction may result in disciplinary action, contractual remedies, account restriction measures, escalation to senior management, external reporting, or termination of employment or relationship, as appropriate. Serious breaches may expose the individual and the Company to civil, criminal, regulatory, and reputational consequences.

25. Effective Date and Approval

This Policy is effective from the date of approval by the Board or authorized governing body of Mento Merkets Ltd. It remains in force until amended, replaced, or withdrawn in accordance with the Company's governance procedures.

Item	Detail
Company	Mento Merkets Ltd.
License Number	2026-00307
Jurisdiction	Saint Lucia
Incorporation Date	15 April 2026
Registered Address	Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia, P.O. Box 838, Castries, Saint Lucia
Policy Owner	Anuj Jayesh sheth
Review Frequency	At least annually, or earlier upon material change

26. Board Approval Block

Approved by: Mento Merkets Ltd.

Board of Directors: Anuj Jayesh Sheth

Approval Date: 11th may 2026

MLRO / Compliance Officer

Name: Meet Y Patel

Date: 11th may 2026

Disclaimer: This Policy has been formally approved by the Board of Directors as recorded below. Approval is evidenced by board resolution, and no physical signature on this document is required for the Policy to be valid and effective.

Version: 1.0

Supersedes: New document