AML/KYC – NPE MARKET

DRAFTED VERSION

1. INTRODUCTION

1.1 This Anti-Money Laundering and Counter-Terrorist Financing Policy ("AML/CFT Policy", "Policy") has been developed by **NPE Market Limited**, a company registered in Saint Lucia under registration number **2024-00497**, having its registered office at Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros Islet, Saint Lucia, and its operational office at The One Tower, 24th Floor, Barsha Heights, Dubai, UAE (hereinafter the "Company").

1.2 The Company is an international provider of online trading services in Foreign Exchange (Forex), Contracts for Difference (CFDs), Metals, Indices, Commodities, Cryptocurrencies and other OTC financial instruments. Due to the nature of these services, the Company is exposed to risks related to money laundering and terrorist financing ("ML/TF") and therefore adopts strict preventive measures.

1.3 This Policy establishes the Company's internal framework for identifying, assessing, mitigating, countering, monitoring, preventing, and reporting ML/TF risks. It operationalizes internal controls, procedures, responsibilities, and monitoring mechanisms aligned with international standards.

1.4 The Policy is binding upon:

- All Company directors
- All employees (permanent, temporary, and outsourced)
- All agents, partners, IBs, affiliates
- All service providers directly involved in KYC/AML processes

1.5 The Company maintains **zero tolerance** toward the use of its products or services for money laundering, terrorism financing, fraud, illegal activity, or abuse.

2. PURPOSE OF THE POLICY

2.1 The main purpose of this Policy is to create a comprehensive AML/CFT regime that aligns with internationally recognized anti-financial crime standards, including but not limited to:

- FATF 40 Recommendations
- Basel AML Index Principles
- Wolfsberg Group Financial Crime Standards
- International best practices for OTC derivatives brokers
- Offshore supervisory norms applicable to financial institutions

2.2 Specifically, this Policy aims to:
a. Prevent the Company from being used for ML/TF or financial crime
b. Ensure a risk-based approach to onboarding, monitoring, and risk-scoring clients
c. Define acceptable and prohibited client activities
d. Establish CDD, SDD, and EDD procedures
e. Establish sanctions screening procedures
f. Ensure timely submission of Suspicious Activity Reports (SARs)
g. Implement strong record-keeping standards
h. Ensure constant staff training
i. Support effective internal audits and AML governance

3. LEGAL & REGULATORY FRAMEWORK

Although registered in Saint Lucia, the Company voluntarily aligns with the highest global AML/CFT standards because it operates internationally, serves clients globally, and uses international banking and payment systems.

The Company's AML/CFT framework is aligned with:

3.1 FATF (Financial Action Task Force) Standards

Including risk assessments, customer due diligence, record-keeping, beneficial ownership identification, sanctions compliance, and reporting obligations.

3.2 International AML Best Practices

Including Wolfsberg Principles, Basel AML Index methodologies, and global brokerage industry AML norms.

3.3 Local Obligations

The Company complies with the AML expectations applicable under Saint Lucia's relevant FIU guidelines, as well as general offshore AML norms required for financial entities.

3.4 Guidance from Other International Regulators

Although not regulated by CySEC, ASIC, FCA, DFSA, or MFSA, the Company voluntarily follows the highest standards across these frameworks to ensure operational integrity, payment-processor acceptance, and global compliance.

4. COMPANY-WIDE AML/CFT GOVERNANCE STRUCTURE

4.1 **Overall Responsibility**
The Company acknowledges that the ultimate responsibility for the prevention of money laundering and terrorist financing rests with the Board of Directors. The Board approves the AML/CFT framework, sets the risk appetite, ensures adequate resources (human, technological and financial), and receives regular reports on the effectiveness of the AML/CFT controls.

4.2 **Board of Directors**
The Board is responsible for establishing and maintaining a strong compliance culture. It must review and approve the AML/CFT Policy, oversee its implementation, and ensure that systems, processes, and personnel are sufficient to identify, manage, and mitigate ML/TF risks. The Board monitors AML performance through periodic reporting, key risk indicators, and internal/external audit findings.

4.3 **AML Compliance Officer (AMLCO)**
The Company appoints a qualified AML Compliance Officer at management level, who acts as the central point of contact on AML/CFT matters. The AMLCO is responsible for:

- Implementing and maintaining the AML/CFT framework.
- Monitoring adherence to this Policy.
- Reviewing and approving high-risk customer relationships and enhanced due diligence cases.
- Assessing and investigating unusual or suspicious activities.
- Determining whether a Suspicious Activity Report (SAR) should be filed.
- Reporting regularly to the Board on AML/CFT issues.
- Ensuring that staff receive relevant training.
- Keeping up to date with changes in laws, regulations and best practices and updating the Policy accordingly.

4.4 **Compliance Department**
The Compliance Department, under the AMLCO, executes day-to-day AML tasks, including performing customer due diligence checks, sanctions screening, transaction monitoring, documentation review, and maintenance of AML files. The department ensures that all onboarding and ongoing monitoring processes conform to this Policy and internal procedures.

4.5 **Operational Departments**
Departments such as Customer Support, Payments, IB/Partnerships and Back-Office play a critical role in AML/CFT. They are required to follow internal procedures, promptly escalate red flags, and cooperate with the AMLCO and Compliance Department during investigations.

4.6 **Independent Audit / Internal Audit Function**
Where applicable, the Company ensures that its AML/CFT systems and controls are subject to independent audit or internal review at regular intervals. The purpose is to test the effectiveness of policies, procedures, monitoring tools, and staff awareness. Findings must be documented, reported to the Board, and remedial actions implemented within defined timelines.

4.7 **Employee Responsibilities**
Every employee, regardless of role, has a duty to be vigilant and to report promptly any suspicion or unusual activity to the AMLCO or the designated AML reporting channel. Failure to comply with AML obligations may result in disciplinary measures, up to and including termination of employment.

5. RISK-BASED APPROACH (RBA)

5.1 **Principle of RBA**
The Company adopts a **Risk-Based Approach** to identify, assess, and manage ML/TF risks. This means resources are allocated proportionately: higher-risk customers, products, or channels are subject to more intensive due diligence and monitoring, while genuinely low-risk situations may attract simplified measures.

5.2 **Firm-Wide Risk Assessment (FWRA)**
The Company performs a Firm-Wide Risk Assessment on a periodic basis (at least annually or upon material changes). The FWRA considers, inter alia:

- Customer types (individuals, corporates, high-risk sectors);
- Products and services (Forex, CFDs, leverage levels, funding methods);
- Geographic exposure (countries of residence, source of funds, i.e. high-risk jurisdictions);
- Delivery channels (online onboarding, IBs, affiliates);
- Payment methods (bank transfer, cards, e-money, payment processors);
- Emerging typologies and regulatory findings.
  The FWRA identify inherent risks, evaluates existing controls, and determines residual risk, which informs the design of AML/CFT controls and risk appetite.

5.3 **Customer Risk Assessment and Scoring**
Each customer is assigned a risk rating (e.g. Low, Medium, High) based on objective and qualitative criteria such as nationality, residence, occupation, SOF/SOW, PE/PEP status, transaction behaviour, and product use. The risk rating determines the depth of due diligence and the intensity of ongoing monitoring.

5.4 **Review and Updating of Risk Assessment**
Risk assessments are not static. The Company periodically reviews risk models, thresholds, and parameters, especially where:

- New products or payment methods are introduced;
- New markets or jurisdictions are targeted;
- Regulatory or FATF publications indicate new risks;
- Internal incidents or suspicious patterns are identified.

6. CUSTOMER ACCEPTANCE POLICY (CAP)

6.1 **General Principle**
The Company will only establish business relationships with customers whose identity is satisfactorily verified and whose activities can reasonably be expected to be legitimate. The Company reserves the absolute right to refuse to onboard any customer, or to terminate an existing relationship, based on AML/CFT grounds and internal risk appetite.

6.2 **Prohibited Customers**
The Company will **not** accept customers who:

- Fail or refuse to provide required identification documents;
- Provide forged, altered or otherwise unreliable documents;
- Are listed on applicable sanctions lists or are known to be associated with terrorism or organized crime;
- Are residents of jurisdictions that are subject to embargoes, international sanctions, or identified as high-risk and non-cooperative by FATF or similar bodies;
- Seek to maintain anonymous or fictitious accounts;
- Insist on unusual secrecy or avoidance of normal communication channels.

6.3 **Customer Acceptance Criteria**
Before accepting a customer, the Company ensures that:

- Full CDD has been conducted and documented;
- The client's SOF/SOW is plausible and commensurate with expected activity;
- There is no positive match in sanctions or negative media screening;
- Any identified risk factors can be adequately mitigated through enhanced controls.

Where high or unmanageable risk is identified, the account will not be opened or will be closed.

7. CUSTOMER DUE DILIGENCE (CDD)

7.1 **Purpose of CDD**
Customer Due Diligence is the process of identifying and verifying the identity of a client and understanding their economic profile in order to assess ML/TF risk. CDD is applied **before** establishing a business relationship and, where appropriate, throughout the course of that relationship.

7.2 **Standard CDD Measures**
Standard CDD includes:

- Identifying the customer's full name, date of birth, nationality, and residential address;
- Verifying identity using reliable, independent documents (e.g. passport, ID card, driving licence);
- Verifying address with acceptable proof (e.g. recent utility bill, bank statement);
- Obtaining information on occupation, employer, and approximate income level;
- Collecting information on the intended use of the trading account (e.g. personal trading, hedging, investment);
- Determining the source of funds (e.g. salary, business income, savings) and, where necessary, source of wealth.

7.3 **Timing of CDD**
As a general rule, CDD must be completed **before** activating the trading account or allowing any trading or withdrawal activity. In strictly controlled cases, the Company may permit limited account functions while verification is in progress, subject to conservative thresholds (e.g. low deposit limits, no withdrawals) and strict timeframes. Failure to complete CDD within such timeframes will result in account suspension or closure.

7.4 **Ongoing CDD and Profile Refresh**
CDD is not a one-off event. The Company periodically reviews and updates customer information, especially when:

- Significant changes occur in trading volume or funding patterns.
- The client updates key profile details.
- Alerts or red flags are raised by monitoring systems.
- Regulatory expectations require re-verification (e.g. after expiry of ID document).

8. ENHANCED DUE DILIGENCE (EDD)

8.1 **Situations Requiring EDD**
Enhanced Due Diligence is applied where the risk is higher, such as:

- Customers from high-risk jurisdictions.
- Politically Exposed Persons (PEPs), their relatives and close associates.
- Customers operating in high-risk industries (e.g. money service businesses, crypto-related firms).
- Unusually complex corporate structures.
- Customers with large or inconsistent transaction volumes relative to their stated profile.

8.2 **EDD Measures**
EDD may include one or more of the following:

- Obtaining additional identification documents or certifications.
- Requesting detailed SOF/SOW evidence (e.g. salary slips, tax returns, business financials, sale contracts).
- Confirming corporate ownership and control structures, including UBOs.
- Conducting deeper adverse media screening and open-source intelligence checks.
- Requiring that first payments originate from a bank account in the customer's name with a reputable financial institution.
- Seeking senior management approval before establishing or continuing the relationship.

8.3 **Approval and Documentation**
All EDD decisions must be documented in the customer file, including the rationale for the risk classification, the additional measures applied, and the final decision (acceptance, rejection, or termination). EDD cases must be reviewed by the AMLCO and, where necessary, escalated to senior management.

9. SIMPLIFIED DUE DILIGENCE (SDD)

9.1 **Conditions for SDD**
Simplified Due Diligence may be applied only in strictly defined circumstances where the ML/TF risk is demonstrably low and there is no suspicion of money laundering or terrorist financing. Even under SDD, the Company must still identify the customer and retain essential information.

9.2 **Scope of SDD**
SDD may involve fewer verification steps or reduced frequency of review but does **not** mean that CDD is completely waived. It may apply, for example, to certain low-risk customers in low-risk jurisdictions with modest transaction volumes and clear SOF/SOW.

9.3 **Prohibition of SDD in High-Risk Situations**
SDD is not permitted where:

- The client is a PEP or related to a PEP.
- The client is from a high-risk or sanctioned jurisdiction.
- The client's activity is inherently risky or complex.
- There is any suspicion or reasonable doubt.

10. BENEFICIAL OWNERSHIP IDENTIFICATION

10.1 **Requirement to Identify Beneficial Owners**
For legal persons and arrangements (e.g. companies, partnerships, trusts), the Company must identify and, where applicable, verify the **ultimate beneficial owner(s)** ("UBO"), being the natural person(s) who ultimately own or control the customer or on whose behalf a transaction is being conducted.

10.2 **Methods of Determination**
The Company obtains corporate documents (certificate of incorporation, share registers, memorandum and articles, etc.) and, where necessary, declarations from directors to establish the ownership structure. All natural persons with a significant ownership or control interest (e.g. ≥10% or as per internal threshold) must be identified and, where required, KYC performed on them individually.

10.3 **Complex Structures and Control Through Other Means**
Where ownership structures are layered, involve nominees, or use offshore entities, the Company must take reasonable steps to trace the ownership to the ultimate natural person(s). Beneficial ownership is not limited to legal shareholding; it may also arise through control rights, voting rights, contractual arrangements, or other means. Relationships that cannot be properly understood or explained may be declined or terminated.

11. ONGOING MONITORING OF BUSINESS RELATIONSHIPS

11.1 **Purpose**
Ongoing monitoring is essential to ensure that customer transactions remain consistent with the Company's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

11.2 **Monitoring Methods**
The Company uses a combination of automated and manual monitoring techniques that may include:

- Threshold-based alerts;
- Pattern recognition (e.g. unusual trading or transfer patterns);
- Behavioural monitoring (e.g. sudden spikes in activity, frequent funding/withdrawal cycles);
- IP address and device monitoring.

11.3 **Examples of Monitoring Criteria**
The Company pays particular attention to:

- Sudden and unexplained increases in deposits or trading volume;
- Frequent deposits followed by immediate withdrawals with little or no trading activity;
- Use of multiple payment methods or accounts not previously declared;
- Repeated attempts to bypass or delay KYC/EDD;
- Activity that does not correspond to the customer's stated profile, occupation or SOF/SOW.

11.4 **Review and Escalation**
Where monitoring flags unusual or potentially suspicious activity, the case is escalated to the Compliance Department and/or AMLCO for review. Additional information may be requested from the customer, transactions may be delayed or blocked, and, where justified, an internal suspicion report may be raised.

12. TRIGGER EVENTS FOR MANUAL REVIEW

12.1 **Definition of Trigger Events**
Trigger events are circumstances or patterns that warrant a manual review of the customer relationship and activity. These events may indicate increased risk, changes in circumstances, or potential misuse of the account.

12.2 **Examples of Trigger Events**
Trigger events include, but are not limited to:

- Change of residence to a higher-risk jurisdiction;
- Change in beneficial ownership or corporate structure;
- Significant increase in trading, deposit or withdrawal volume without clear economic rationale;
- Receipt of negative media information about the customer;
- Use of VPNs, proxies or other obfuscation tools to hide location in a suspicious manner;
- Requests for unusual withdrawal routing (e.g. different currencies, multiple third parties);

- Internal or external requests for information from regulatory, law enforcement, or banking partners.

12.3 **Handling Trigger Events**
Upon a trigger event, the Company conducts enhanced review, which may include:

- Re-confirmation of identity and address;
- Requesting updated SOF/SOW evidence;
- Imposing temporary restrictions on account activity;
- Re-assessment of risk rating;
- Decision whether to continue, restrict or terminate the relationship.

13. SUSPICIOUS ACTIVITY REPORTING (SAR)

13.1 **Duty to Report**
Any employee who identifies or suspects that funds or activity may be linked to money laundering, terrorist financing, fraud, or any other financial crime must report the suspicion without delay to the AMLCO or the designated reporting channel, in accordance with internal procedures. This duty exists regardless of transaction amount.

13.2 **Assessment of Suspicion**
The AMLCO examines internal reports, reviews supporting documentation, and determines whether the suspicion is justified. Where appropriate, the AMLCO may request additional information from internal systems or from the customer, provided that such request does not amount to “tipping-off”.

13.3 **Filing SARs with Authorities**
If the AMLCO reasonably believes that activity may be linked to ML/TF or related offences, a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) is submitted to the relevant Financial Intelligence Unit or competent authority in accordance with applicable law. The customer must not be informed of the SAR filing.

13.4 **Post-Reporting Measures**
Following SAR submission, the Company may:

- Freeze or restrict the customer’s account;
- Decline to process further transactions;
- Terminate the business relationship;
- Co-operate fully with law enforcement.

14. PROHIBITED ACTIVITIES AND PRACTICES

14.1 **Anonymous or Fictitious Accounts**
The Company strictly prohibits anonymous, fictitious, or numbered accounts. All relationships must be fully identifiable and documented.

14.2 **Third-Party Payments (Unjustified)**
Deposits or withdrawals from/to unrelated third parties are generally not permitted unless specifically justified, documented, and approved under EDD procedures (e.g. corporate accounts, verified related parties). Suspicious third-party payments are rejected and may be reported.

14.3 **Use of the Trading Account as a Payment Channel**
The trading account may not be used as a general payment/transfer facility. The Company does not permit customers to route unrelated third-party funds via its accounts without genuine trading activity.

14.4 **Use of False or Forged Documents**
The provision of false, altered, or counterfeit documents is strictly prohibited and may result in immediate account closure, SAR filing, and possible reporting to authorities.

14.5 **Use of High-Risk Payment Methods Without Transparency**
Deposits via high-risk payment methods, including opaque e-wallets or crypto channels, may be limited, restricted, or prohibited, particularly when traceability and SOF are unclear.

15. RECORD KEEPING

15.1 **Retention Period**
The Company keeps all AML relevant records for a minimum of **five (5) years** after the end of the business relationship or the date of the last transaction, whichever is later, or longer if required by applicable legislation or for the defence of legal claims.

15.2 **Scope of Records**
Records include, but are not limited to:

- KYC documents and verification evidence;
- Economic profile and risk assessment;
- Transaction and trading history;
- Payment details (deposits/withdrawals);
- Internal reports and SAR documentation;
- Correspondence with the customer relating to AML/CFT issues;
- Training records and AML program reports.

15.3 **Format and Accessibility**
Records may be held in physical or electronic form, provided they are secure, accurate and retrievable in a timely manner for regulatory, audit, or investigative purposes. The Company implements appropriate safeguards against unauthorized access, alteration, or destruction.

16. PERSONNEL EDUCATION AND TRAINING

16.1 **Objective of Training**
The Company ensures that all relevant staff understand ML/TF risks, their personal responsibilities, internal procedures, and the consequences of non-compliance. Training enables employees to recognize red flags and handle customer interactions in compliance with AML/CFT obligations.

16.2 **Scope of Training**
Training programs cover, at minimum:

- Basic concepts of money laundering and terrorist financing;
- Relevant legal and regulatory obligations;
- Company policies and procedures;
- Customer acceptance and CDD/EDD requirements;
- Identification of suspicious activities and red flags;
- Reporting channels and protection of reporters;
- Sanctions compliance;
- Case studies and practical scenarios.

16.3 **Frequency and Tailoring**
New staff receive induction training upon joining. Thereafter, refresher training is provided at regular intervals (e.g. annually) or when material changes occur in laws, regulations, products, or risk exposure. Training content is tailored to departmental roles (e.g. support, payments, IB management, IT).

16.4 **Records of Training**
The Company maintains records of all training sessions, including dates, participants, topics covered, and materials used, for audit and supervisory review.

17. INDEPENDENT REVIEW / AUDIT

17.1 **Purpose**
An independent review or internal audit of the AML/CFT framework is carried out periodically to assess whether policies, procedures and controls are adequate and effective in managing ML/TF risks.

17.2 **Scope**
The review assesses:

- Compliance with this Policy;
- Quality of CDD/EDD documentation;
- Effectiveness of sanctions screening and monitoring tools;
- Quality and timeliness of suspicious activity reporting;
- Adequacy of training and awareness;
- Implementation of previous audit recommendations.

17.3 **Reporting and Remediation**
Findings from the review are communicated to the Board and AMLCO, and an action plan is prepared to address any weaknesses identified. Progress on remediation is monitored until completion.

18. TECHNOLOGY, SYSTEMS AND CONTROLS

18.1 **Use of Technology**
The Company employs technological solutions to support efficient and effective AML/CFT controls, including automated KYC tools, sanctions screening engines, transaction monitoring systems, and risk-scoring models.

18.2 **System Calibration and Maintenance**
Systems are calibrated to reflect the Company's risk appetite and updated regularly to address emerging threats, regulatory changes, and new products. Parameters such as thresholds, risk indicators, and alert rules are periodically reviewed and tested.

18.3 **Human Oversight**
Technology does not replace human judgement. Alerts and system outputs are reviewed by trained staff, and decisions on high-risk or complex matters are escalated to senior compliance personnel or the AMLCO.

19. RELATIONSHIP WITH INTRODUCING BROKERS (IBs) AND PARTNERS

19.1 **Role of IBs and Partners**
IBs and partners may introduce customers to the Company. However, IBs and partners do **not** relieve the Company of its responsibility to perform its own AML/CFT obligations.

19.2 **Due Diligence on IBs**
The Company performs due diligence on IBs and partners to understand their business,

reputation, regulatory status (if any), and AML controls. High-risk IBs may be rejected or subject to additional oversight.

19.3 **Responsibilities of IBs**
IBs must:

- Not engage in any activity that facilitates ML/TF;
- Not misrepresent the Company's services;
- Not handle client funds unless explicitly authorized and properly regulated;
- Co-operate fully with the Company's AML/CFT requirements;
- Immediately report any suspicious conduct by their referred clients.

19.4 **Monitoring and Termination**
The Company monitors IB-related activity for unusual patterns (e.g. clusters of high-risk clients, repeated bonus or promotion abuse). The Company reserves the right to suspend or terminate IB agreements where AML/CFT concerns arise.

20. REFUSAL OR TERMINATION OF BUSINESS RELATIONSHIPS

20.1 **Right to Refuse**
The Company reserves the right to refuse to open an account or to provide services where AML/CFT concerns cannot be mitigated, or where the customer fails to satisfy CDD/EDD requirements.

20.2 **Right to Restrict or Terminate**
The Company may freeze, restrict, or terminate an existing relationship if:

- There is a suspicion of ML/TF;
- The customer refuses to provide additional information or documents;
- The customer is identified on a sanctions list;
- The customer engages in abusive, fraudulent or deceptive behaviour;
- Requests of competent authorities require such action.

20.3 **Non-Liability**
To the maximum extent permitted by applicable law, the Company bears no liability for losses or damages incurred by any person as a result of measures taken in good faith to comply with AML/CFT obligations, including refusal, restriction, or termination of services.

21. REVIEW AND AMENDMENT OF THIS POLICY

21.1 **Periodic Review**
This AML/CFT Policy is reviewed at least annually, or more frequently if required by changes in business model, regulatory expectations, FATF guidance, or identified deficiencies.

21.2 **Amendments**
The Board approves material changes to this Policy, based on recommendations from the AMLCO and senior management. Updated versions are communicated internally and, where relevant, made available to stakeholders.