Know Your Customer Policy (the “KYC Policy”)

BIGIDEA NETWORK FZ-LLC

1. Introduction

BIGIDEA NETWORK FZ-LLC (the “Company”) adheres to strict standards in client identification and verification, which form an integral part of its Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) framework and this KYC Policy.

The Company has implemented KYC procedures in accordance with the applicable laws and regulations of the United Arab Emirates, including Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing, Cabinet Resolution No. (134) of 2025, and international standards issued by the Financial Action Task Force (FATF).

---

2. Objectives of the KYC Policy

The main objectives of this KYC Policy are:

a) to ensure compliance with applicable UAE AML/CFT laws and regulatory requirements related to client identification and verification;
b) to mitigate risks associated with money laundering, terrorist financing, fraud, and other illegal activities;
c) to maintain a high level of trust through transparent and secure internal control procedures;
d) to protect the interests of Clients and ensure the security and confidentiality of their data.

---

3. Key Stages of the KYC Procedure

The Company applies a risk-based approach to client onboarding and monitoring, which includes the following stages:

a) provision of KYC information and documents;
b) client verification;
c) risk assessment and decision-making;
d) ongoing monitoring and control.

3.1. Provision of KYC Information and Documents

The Company identifies each Client prior to establishing a business relationship.

For this purpose, the Client shall:

a) complete required information via the KYC questionnaire;
b) provide valid KYC documents and supporting information.

The collected data may include, but is not limited to:

- **For individuals:** full name, date of birth, residential address, email address, phone number, and identification details;
- **For legal entities:** company name, registered address, contact details, website, business activity description, ownership structure, and information on directors, Ultimate Beneficial Owners (UBOs), and authorized persons.

Examples of KYC documents include:

- **For individuals:** passport or ID and proof of address (e.g. utility bill or bank statement not older than 3 months);
- **For legal entities:** certificate of incorporation, memorandum and articles of association, business license, shareholder register, proof of domain ownership, and documents confirming appointment of directors.

The Company may request additional documents where necessary, including in higher-risk cases.

All documents must be valid, clear, and, where applicable, translated into English (with notarization if required).

3.2. Client Verification

All KYC documents and information provided are subject to verification.

Verification procedures include:

- validation of documents authenticity;
- verification of business activity and website functionality;
- screening against sanctions lists, PEP databases, and adverse media;
- assessment of the Client’s reputation and background.

3.3. Risk Assessment and Decision-Making

Following verification, the Company assesses the risk level associated with each Client based on factors including:

a) geographic location (including high-risk jurisdictions);
b) nature of business activities (including high-risk industries);
c) ownership structure and transparency;
d) Politically Exposed Person (PEP) status;
e) transaction patterns and any suspicious activity indicators.

Clients are assigned a risk rating (Low, Medium, High).

High-risk Clients may be subject to Enhanced Due Diligence (EDD), including additional verification and monitoring.

Based on the risk assessment, the Company may approve or reject the Client. The Company reserves the right to refuse or terminate services if:

- required information is not provided;
- information is false, misleading, or inconsistent;
- there are AML/CFT or sanctions-related concerns.

Where suspicion arises, the Company will submit a Suspicious Activity/Transaction Report (SAR/STR) to the UAE Financial Intelligence Unit (FIU) via the goAML system, in accordance with applicable regulations.

3.4. Monitoring and Ongoing Control

The Company conducts ongoing monitoring of Client relationships and transactions to detect unusual or suspicious activities.

Client information is regularly reviewed and updated to ensure accuracy and relevance. This may include:

a) periodic review of Client data;
b) re-verification of identity and/or source of funds/wealth in case of changes in Client behavior or risk profile.

---

4. Duties and Responsibilities of Employees

All employees involved in KYC and AML/CFT processes are required to:

a) comply with internal KYC and AML/CFT procedures;
b) remain vigilant to potential indicators of suspicious activity;
c) promptly report any concerns regarding Client information or behavior to the designated Compliance Officer;
d) undergo regular AML/KYC training.

Failure to comply with these requirements may result in disciplinary action.

---

5. Conclusion

The Company maintains high standards of transparency, security, and compliance.

All Client data collected under KYC procedures is treated as confidential and used solely for compliance with legal and regulatory obligations and prevention of financial crime. Information may be disclosed only where required by law or with Client consent.

All KYC records and related documentation are retained for at least **five (5) years** following the termination of the business relationship, in accordance with UAE regulations.

The Company reserves the right to update this KYC Policy in response to regulatory or operational changes.

For further information, please contact: compliance@bigidea-network.com