AML POLICY

UICOM – FZCO

1. INTRODUCTION

1.1. This Anti-money laundering Policy is the basic standards of Anti-Money Laundering and Combating Terrorism Financing (hereinafter collectively referred to as – "Policy") procedures of UICOM–FZCO, company registered in the UAE, license number 47789, registration address: Office A2, Dubai Silicon Oasis, DDP, Dubai, United Arab Emirates, (hereinafter collectively referred to as – "Company").

1.2. FZCO acts in its capacity in terms of international standards: recommendations and papers from the Financial Action Task Force (FATF), European regulations related to AML/CFT: "Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing", "Regulation 2015/847 on information accompanying transfers of funds", Anti-money laundering (AMLD V) - Directive (EU) 2018/843, Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations (as amended by Federal Decree Law No. (26) of 2021), Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (as amended by Cabinet Resolution No. (24) of 2022) etc.

1.3. This Policy is valid, and copies of this Policy will be distributed to all required persons, and all responsible employees must be aware of the materials contained in this Policy and use them in all cases.

1.4. It is the Policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities in all our services. In accordance with the Company's Policy, we comply with all applicable AML Laws in all transactions carried out our service. To this end, the Company will cooperate and work exclusively with clients who are involved in legitimate business activities and whose funds are obtained from legitimate sources.

1.5. Company respects and is committed to applying all internal (by-laws) laws and regulations, as well as special measures, to prevent money laundering and terrorist financing worldwide.

1.6. For the purposes of this Policy, unless the context shall prescribe otherwise:

"Business Relationship" means a business, professional or commercial relationship which is connected with the professional activities of the Company and which was expected, at the time when the contact was established, to have an element of duration.

"Client" or "User" means any legal or physical person aiming to conclude a Business Relationship or conduct a single transaction with the Company. Counterparties are also treated as Clients only when

the Company is executing a Client order by entering into a dealing in securities transaction directly with the Counterparty.

2. KEY STAGES OF MONEY LAUNDERING

2.1. There are many ways to launder money in accordance with legal regulations.

Money laundering methods are divided into three distinct stages:

- Placement– this is the first stage in the money laundering operation and involves the physical disposal of the initial proceeds derived from illegal;
- Layering– this second stage involves separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity;
- Integration– the final stage involves providing an apparent legitimacy to the criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

Money Laundering has the following meaning: participation in actions that are deliberately aimed at concealing or concealing true origin of funds obtained by criminal means, with the aim of making these proceeds appear to be derived from legal origin or constitute legal assets.

2.2. The following types of activities are "money laundering" and are prohibited under this Policy:

a) transfer of ownership of funds (activities), knowing or suspecting that such activities was obtained as a result of criminal or certain illegal activities, with the aim of concealing the illegal origin of funds (activities), or assisting any person involved in such activities in evading the legal consequences of his actions;

b) the commission of any financial transactions using funds (activities) obtained by criminal means;
c) concealment of the true nature, source, location, movement, rights in relation to the possession or control of criminal funds (activities);

d) acquisition, possession or use of assets by criminal means;

e) assistance in the implementation of illegal activities;

f) participation, complicity in committing, attempts to commit and aiding, abetting, helping, and advising in the commission of any of the actions mentioned above.

2.3. By the broader definition of Money Laundering, we mean that any person, including but not limited to any employee of the Company, can break the law if he/she becomes aware of or suspects the existence of criminal activities within the framework of his /her business and becomes involved or continues to accept participating in a matter which relates to that property being linked to the business without reporting his/her concerns.

2.4. The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. The Company shall assess and evaluate the risks it faces, for the use of the Dealing in Securities and Ancillary Services for the purpose of Money Laundering or Terrorist Financing. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services and the financial instruments that the Company provides are relatively simple, involving relatively few Clients or Clients with similar characteristics, then the Company shall apply such procedures which are able to focus on those Clients who fall outside the 'norm'.

2.5. Company Risks.

The following, inter alia, are sources of risks which the Company faces with respect to

Money Laundering and Terrorist Financing:

(a) Risks based on the Client's nature:

- complexity of ownership structure of legal persons;
- companies with bearer shares;
- companies incorporated in offshore centers;
- PEPs;
- Clients engaged in transactions which involves significant amounts of cash;
- Clients from high risk countries or countries known for high level of corruption or organized crime or drug trafficking;
- unwillingness of Client to provide information on the Beneficial Owners of a legal person.

(b) Risks based on the Client's behavior:

- Client transactions where there is no apparent legal financial/commercial rationale;
- situations where the origin of wealth and/or source of funds cannot be easily verified;
- unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

(c) Risks based on the Client's initial communication with the Company:

- Clients using third parties identification /or nickname;
- Clients introduced by a third person.

(d) Risks based on the Company's services and financial instruments:

- services that allow payments to third persons/parties;
- large cash transactions.

3. POLICY STATEMENT ON AML

3.1. This Policy is designed to notify all employees, contractors, partners, members, clients and other third parties acting on behalf of the Company about major and potential violations of anti-money laundering laws and to support them in making the right decisions in accordance with our corporate position as set out in this Policy.

This Policy is binding and applies to all, without exception, the Company's operations around the world, including but not limited to all worldwide owned legal entities or controlled by the Company, as well as to all directors, officers, employees, key-employees, contractors, partners, clients and other third parties acting on behalf of the above.

The internal structure of the Company and its compliance department are designed to combat money laundering and terrorist financing, which cover the following aspects:

3.1.1. The development of robust internal policies, procedures and controls that strive to combat any attempted use of Company products for illegal or illicit purposes and to ensure our customer's protection under the relevant laws and regulations. This includes identification customer/contractor, including appropriate screening and application of enhance due diligence where applicable, keep adequate records, compliance with all applicable rules for the processing of personal data, including GDPR, Bribery and Corruption, Code of Conduct related areas, IT security, dealing with customer's/contractor's, review and assessment of the internal policies and procedures.

By providing your data to the Company, you undertake the following obligations:

- you warrant and represent that you will comply with all applicable anti-money laundering and anti-terrorist financing laws and regulations, including, but not limited, the AML Policy.
- you warrant and acknowledge that you do not own the information and/or have no suspicion that the funds in the past, present or future are obtained from an illegal source or have anything to do with money laundering, or other illegal activities prohibited by applicable European and UAE laws, including the laws and regulations of any international organization;
- you confirm and agree to immediately provide the Company with any necessary information that we deem necessary to request, in order to comply with applicable laws and regulations in relation to anti-money laundering;
- company collects and stores documents proving the identity of the Client, as well as reports on all transactions made on the account within 5 years, and for at least five years from the date on which the business relationship is terminated;

- company monitors suspicious transactions on the account of the Client, as well as transactions carried out under special conditions;
- company reserves the right at any time and at any stage to refuse the Client to carry out an operation if the Company has reason to believe that this operation has anything to do with money laundering and criminal activity.

Based on the legislative norms and rules provided for by international law, the Company is not obliged to notify the Client that his activity is suspicious, and information about it has been transferred to the relevant state authorities.

Following the internal AML Policy, the Company is obliged to conduct initial and ongoing identity (Normal Due Diligence and Enhanced Due Diligence) checks of all Clients, in accordance with all levels of potential risk (Low Risk, Medium Risk, Hight Risk).

A) Low Risk Clients

The Company shall accept Clients who are categorized as low risk Clients as long as the general principles under Section 3.1.2. are followed.

Moreover, the Company shall follow the Simplified Client Identification and Due Diligence Procedures for low risk Clients.

B) Normal Risk Clients

The Company shall accept Clients who are categorized as normal risk Clients as long as the general principles under Section 3.1.2. of the Policy are followed.

C) High Risk Clients

The Company shall accept Clients who are categorized as high risk Clients as long as the general principles under Section 3.1.2. of the Manual are followed.

Moreover, the Company shall apply the Enhanced Client Identification and Due Diligence measures for high risk Clients and the due diligence and identification procedures for the specific types of high risk Clients mentioned as well as applicable.

D) Not Acceptable Clients

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship or an execution of an Occasional Transaction with the Company:

- Clients who fail or refuse to submit, the requisite data and information for the verification of his identity, residential address and the creation of his economic profile, without adequate justification;
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form;
- Clients who are involved in electronic gambling/gaming activities through the internet;
- Clients in the list of Restricted Businesses (Appendix 1)
- Clients who are residents of the list of prohibited countries (Appendix 2)

3.1.2. The Company shall duly apply Client identification procedures and Client due diligence measures in the following cases:

(a) when establishing a Business Relationship

(b) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction

(c) when there are doubts about the veracity or adequacy of previously Client identification data.

d) as well as in cases provided for in Section 4.5. of this Policy.

Client identification documents and relevant information shall be updated on an annual basis or earlier if deemed necessary (e.g. in case of investigation of suspicious transactions etc.)

3.1.3. In order to prevent possible online fraud, we reserve the right at any time to verify the authenticity of your credentials, such as your name, address, age and payment methods that you use, requiring you to submit all the necessary documents for this verification.

These documents usually include proof of your identity, your residential address (such as a utility bill), and the method of payment you are using.

3.1.4. IDENTITY DOCUMENTS:

1. Photo ID. This could be a copy of your passport, driver's license, or other proof of your identity. To verify your identity, we require a photo of your identity document.

2. Proof of Address: For this purpose, you can send us your utility bill or credit card statement. This document should be recently received by you, and it should clearly show your full name and address.

3. Notarized Documents: Your documents must be certified by the signature and stamp of an authorized notary / legal counsel to prove the legality of the documents you provide.

3.1.4.1. Attention! In some cases, depending on the method of payment that you used to make a deposit/payment, you may be asked to provide one or more of the above documents or other additional documents not included in this list.

3.1.5. The Client undertakes to provide information within 48 hours of receiving the request. We reserve the right not to report successful verification results.

3.1.6. If the Client refuses or ignores our request to provide these documents, the Company may, at its sole discretion, refuse to provide services.

3.1.7. If the documents you send us do not pass our internal security checks, for example if we suspect that you have sent us fraudulent documents, or that your documents contain falsified information or have been provided to us for the purpose of misleading, we will not must treat these documents as legitimate and inform you about this decision.

4. CLIENT IDENTIFICATION PROGRAM

4.1. The company will take all reasonable steps to establish the identity of any person invited to provide its services (hereinafter referred to us Users/Clients).

4.2. For this, the registration process of Users/Clients, provided for in the Terms and Conditions of the Company, provides Due Diligence, which must be carried out before the opening of the User/Client account.

4.3. The Company is obliged to collect necessary identification information about each User/Client who registers on the website and creates an account.

The company may ask for the following information:

- date of birth of the User/Client (in accordance with applicable laws, we establish the requirement for the User/Client to be over eighteen (18) years old);

- the name and surname of the User/Client;

- place of residence of the User/Client;

- a valid email address of the User/Client;

- username and password applicable on our website.

4.4. The Company may also require any User/Client to provide other additional information and/or documentation. In certain cases, the Company may require the User/Client to provide notarized copies of documents.

4.5. Documents to verify the identity information received will be requested from each User/Client if and when there is considered to be risk or uncertainty about the information provided and prior to any payment in excess of EUR 1 000,00 and above per occasion or when payments to the account are made in excess of EUR 1 000,00 and above.

These documents shall include, to the extent permitted under the relevant data protection regulations:

- copy of valid ID or Passport;

- proof of address.

4.6. The Company must, within the prescribed period (within 2 business days) after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.

5. KEY POINTS OF THE COMPANY:

5.1. Appoint Money Laundering Reporting Officer (hereinafter referred to us - MLRO) to whom a report is to be made about any information or other matter which proves or creates suspicion that person is engaged in a money laundering offence or terrorist financing according to the) Prevention and Suppression of Money Laundering Activities and Terrorist Financing laws of 2007 and 2018 (No 13(I) 2018).

5.2. Implement risk sensitive policies and procedures relating to all client/user due diligence, reporting, record keeping, internal control, risk assessment and management, monitoring and management of compliance, along with the communication of policies and processes.

5.3. All employees must be vigilant for the signs of money laundering.

5.4. Any employee who suspects money laundering activity must report this promptly to the Compliance Person (MLRO) as the officer delegated to receive such reports.

5.5. According to the provision 16 of "Regulation 2015/847 of the European parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006", the Company has the obligation to check whether information on the payer or the payee is accurate should, in the case of transfers of funds where verification has not yet taken place, be imposed only in respect of individual transfers of funds that exceed EUR 1 000, unless the transfer appears to be linked to other transfers of funds which together would exceed EUR 1 000, the funds have been received or in anonymous electronic money, or where there are reasonable grounds for suspecting money laundering or terrorist financing. This amount refers to the actual value that crosses the border and excludes any fees that may be applicable to that transaction.

6. COMPLIANCE PERSON (AML COMPLIANCE PERSON)

6.1. The Company has designated AML Compliance Officer (with full responsibility for the Company's AML program.

6.2. The Company is obliged to register the MLRO and Compliance Officer in registration system called AML according to all requirements of Directive (EU) 2015/849 and other AML Directives. The duties of the Compliance Officer will include monitoring the Company's compliance with AML

obligations, overseeing communication and training for employees according to Directive (EU) 2015/849. Compliance Officer will also ensure that the Company keeps and maintains all of the required AML records. Compliance Officer is vested with full responsibility and authority to enforce the Company's AML program.

7. TRAINING PROGRAM

7.1. Company is committed to providing ongoing training for all its employees under the guidance of an MLRO and senior management. The training will be held at least once a year. The training process may change, depending on the conversion of the base of Users/Clients, the resources of the Company, and will be updated as necessary to reflect any new changes in the legislation.

7.2. The training will include, at a minimum:

• how to identify high-risk clients and the signs of money laundering arising in the performance of duties by employees;

• what actions should be taken after risk identification (step-by-step instructions on communication with the Compliance Department, with knowledge of the rules for reporting unusual activity of any User/Client or other red flags for analysis;

• the policy of the Company for the storage of the documentation of Users/Clients;

• disciplinary action for non-compliance with applicable law.

8. SUSPICIOUS TRANSACTIONS AND REPORTING

8.1. According to the Chapter II, article 5 of Regulation (EU) 2015/847 of The European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, Money Laundering Reporting Officer will report any suspicious transactions (including deposits and transfers) conducted or attempted by, at or through a User/Client account involving EUR 1 000,00 and above of funds (either individually or in the aggregate) where the AML Compliance Person knows, suspects or has reason to suspect:

- User/Client is included on any list of individuals assumed associated with terrorism or on a sanction list;

- The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation;

- The transaction has no ordinary lawful purpose or is not the sort in which the User/Client would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or

- The transaction involves the use of the Company to facilitate criminal activity.

9. COMPLIANCE CONTROLS

9.1. The management of the Company is committed to complying with all laws mentioned above. Any employee or Client/ User who violates the rules in this Policy or who permits anyone to violate those rules may be subject to appropriate disciplinary action, up to and including dismissal, and may be subject to personal civil or criminal fines.
9.2. Company is responsible for ensuring that business has a culture of compliance and effective controls to comply with European and the UAE related laws, with the main provisions of The Prevention and Suppression of Money Laundering and Terrorist Financing Law, the AML Directives issued from CySEC and regulations to prevent, detect and respond to money laundering and counter-terrorism financing and to communicate the serious consequences of non-compliance to employees.

9.3. You have the obligation to read and follow this Policy. Any Company's employee or contractor, partner who violates this Policy may be subject to appropriate disciplinary action, independently from potential other penalties resulting from their behavior.

9.4. This Policy will be updated in accordance with legal requirements and innovations, and the updated version of the Policy will be immediately available on the Company's intranet

10. FURTHER INFORMATION

10.1. This Policy shall be governed by and interpreted in accordance with the laws of the United Arab Emirates, as well as international legal acts.

10.2. Each clause contained in this Policy shall be separate and severable from each of the others. If any clause is found to be void, invalid, or unenforceable for any reason whatsoever, the remaining clauses shall remain in full force and effect.

If you have any questions about this Policy, you should contact the Compliance Department. Further information can be obtained from the following sources:

Email: company@uicom.ae

Website: https://uicom.ae

APPENDIX 1

LIST OF RESTRICTED BUSINESSES

Businesses that offer illegal products or services are never eligible to use UICOM–FZCO services.

Prohibited Products and Services:

1. Adult entertainment, website or contents such as:

- "Pay sites", which require money from the user to access adult content;
- "Free sites" (such as TGP, MGP, tube sites or affiliate sites) which provide free access to adult content;
- "Live webcam sites" which allow users to interact with performers using webcam and chat technology;
- "Clip sale sites" which allow content producers to upload and sell their own adult video clips;
- "Adult dating sites" which connect individuals interested in erotic social interaction;
- Sexually oriented items such as sex toys;
- Adult escorts, prostitution services and massage parlours;
- Child pornography;
- Male or Female Sexual Enhancement Supplements or Products;
- Video texting or paid subscriptions to live-streaming where it involves adult erotic content or conversations;
- Gentleman's Clubs, Strip Clubs and Topless Bars;
- Mail order brides services.

2. Drugs, medical marijuana, cannabis seeds, drug paraphernalia such as:

- Drugs or drug proprietors selling illegal substances;
- Drug paraphernalia that involves equipment designed for making or using drugs;

3. Tobacco / Cigar / Electronic Cigarette / Nicotine content products.

4. Illegal substances and products such as:

- Espionage equipment and accessories;
- Jail breaker equipment and software;
- Hacking and cracking materials e.g. Malware, Software to break encryption of phones/computers;
- Signal Jammers/Blockers that interferes with cellular/communication devices;
- Fake credentials, fake academic papers, etc.
- Illegal sale of financial information (e.g. bank accounts, bank cards);
- Stolen goods including digital and virtual goods;
- Counterfeit products and replicas;
- Poisonous and hazardous materials.

5. Trade of weapons, ammunition, military arms, explosive devices and firearm parts.

6. Unauthorized copyright media and software such as Illegal downloads of movies, music, computer and video games.

7. Human organs, remains and body parts.

8. Surrogacy services.

9. Illegal investment schemes, including Pyramid or Ponzi schemes.

10. Merchants involved with bestiality, rape, hate, violence, or incest.

11. Products/Services promoting abuse, hatred, racism, religious persecution, terrorism, violence or contain offensive content.

12. Sanction list inclusions (global).

13. Any other category, products or services that Impex Trading Limited decides to prohibit, in its sole discretion.

Also, some industries are more liable to fraud than others. That is why we are not allowed to accept the following companies to prevent any criminal activity and money laundering:

1. Get rich schemes.

2. Gambling providers or transactions including games of chance.

3. Ticket brokers.

4. Precious metals/materials.

5. Telemarketing companies.

6. 3rd party/aggregation.

7. Collection agencies.

8. Payday lenders.
9. Credit repair companies.
10. Loan modification.
11. PPI claims.
12. Penny auctions.
13. Tattoo Parlours.