Anti-Money Laundering (AML) Program

1. Purpose

The purpose of this directive is to prevent money originating from criminal activity or illegally obtained assets (money laundering) from being introduced into the economic cycle through GULF BROKERS LTD, Registration No. 8417634-1, Reg. address: Room B11, First Floor, Providence Complex, Providence, Mahe Seychelles. PO BOX 6007 (hereinafter called the "Company"), while both:

a) THE YORK MANAGEMENT DMCC, Reg. address Unit No. 506, Cluster C, Gold Crest Executive, Plot No. JLT-PH1-C2A, Jumeirah Lakes Tower, Dubai, United Arab Emirates and
b) THE YORK MANAGEMENT INC, Corporation No. 71638, Reg. address Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, MH96960, Marshall Island,

acting as Company´s marketing partners.

In addition, this Program also serves to prevent terrorist financing by ensuring that financial flows to which terrorists could have access are sufficiently protected against any such access. Terrorist financing is when money or other means are used to commit terrorism or to support terrorist organizations.

Money laundering and terrorist financing are punishable by imprisonment in many countries of the world, as well as fines against companies or their employees. In addition to money laundering requirements in other legal systems, companies are required to take preventive measures against money laundering and terrorist financing under the Anti-Money Laundering Act.

This corporate directive establishes binding standards applicable, process basics, as well as essential tasks within the scope of work of the contact person for the prevention of money laundering (contact person for AML) for the effective prevention and fight against money laundering. In addition to the implementation of legal requirements, it also serves to specify the principles of behavior for the purposes of effective and sustainable money laundering prevention.

Relevant national legislation takes precedence over this directive, or apply in addition to this directive if they contain different, additional or additional modifications or stricter measures.

This program applies to every entity related to the Company, and its employees, directors, officers, contractors, or any third party working on behalf of the company.

The policy is for internal use, and the administration is required to convey it to every concerned person or entity. Failure to comply with the policy will result in appropriate action.

2. Introduction and application of this Program

2.1. OCTRADO is a registered brand name of GULF BROKERS LTD, Registration No. 8417634-1, Reg. address: Room B11, First Floor, Providence Complex, Providence, Mahe Seychelles. PO BOX 6007 (hereinafter called the "Company") to its clients (hereinafter called the „Users") used mainly through its webpage https:// https://octrado.com/, while both:

a) THE YORK MANAGEMENT DMCC, Reg. address Unit No. 506, Cluster C, Gold Crest Executive, Plot No. JLT-PH1-C2A, Jumeirah Lakes Tower, Dubai, United Arab Emirates and
b) THE YORK MANAGEMENT INC, Corporation No. 71638, Reg. address Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, MH96960, Marshall Island

acting as mere marketing partners.

2.2. This Policy applies to all Employees of the Company, including those working with Company on a purely voluntary basis. Company will terminate its involvement with any Employees who fail to comply with this Program.

3. Money Laundering and Terrorist financing

3.1. Money Laundering („ML“)

a) the term “money laundering” refers to an act intended to have the effect of making any “property” (defined broadly to include any tangible or intangible financial benefit) that represents the proceeds obtained from the commission of a crime appear not to represent such proceeds. Put another way, money laundering is the process of disguising or “cleaning” money directly or indirectly arising from criminal activity (i.e. “dirty money”) so as to conceal its criminal origins.

b) ML generally consists of three common stages:

(i) **placement** - the physical disposal of cash proceeds derived from illegal activities into the financial system, or conversion of funds already in the financial system into the proceeds of crime (e.g. tax evasion, payments made for corrupt or criminal purposes);

(ii) **layering** - separating illicit proceeds from their source by creating complex layers of financial transactions, often with no legitimate commercial purpose, designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

(iii) **integration** - returning the laundered proceeds back into the general financial system in a way so that they appear to be the result of, or connected to, legitimate business activities.

c) The primary ML offences under relevant criminal law:

(i) **“Dealing” with criminal property**: it is an offence for a person who, knowing or having reasonable grounds to believe that any property which, in whole or in part, directly or indirectly represents the proceeds of crime, “deals” with that property. “Dealing” covers a wide range of activity, including receiving or acquiring, concealing or disguising, disposing or converting, or using the property as security (e.g. for a loan).

(ii) **Failure to disclose**: it is an offence for a person who knows or suspects that any property (in whole or in part, directly or indirectly) represents the proceeds of crime or was otherwise used, or is intended to be used, in connection with an indictable offence, to fail to disclose that knowledge or suspicion to an authorized

officer as soon as it is reasonable to do so. In other words, there is a statutory "duty to report" knowledge or suspicion of ML.

(iii) **Tipping off**: it is an offence for a person who knows or suspects that a report has been made under sub-para (ii) to disclose that fact to any other person (e.g. to the individual suspected of being involved in ML) in a manner which is likely to prejudice any investigation which might be conducted by law enforcement as a result of the original report.

3.2. For purposes relevant to this Program Terrorist Financing („TF") shall mean an occasions when funds from either legitimate or criminal sources (or a combination of the two) are used to encourage, plan, organize, or commit a terrorist act, participate or threaten to participate in terrorist activities, or to otherwise benefit a terrorist or terrorist organisation. In TF, the focus is on the end use of the funds in question, whereas with ML, the focus is on the origin of the funds.

4. Authority for prevention of Anti-Money Laundering

4.1. In the area of Compliance, a central body for the prevention of money laundering has been established. This authority is referred to as the Anti-Money Laundering Compliance officer (hereinafter abbreviated as "AML-Co"). AML-Co is responsible for setting standards and coordinating measures necessary to prevent money laundering within the scope of this directive. The role of the AML-Co is to regularly exchange information with the person responsible for the prevention of money laundering and is available to him as an advisory body.

4.2. AML-Co is body responsible for implementation of this Program.

4.3. If anyone in the company knows or suspects that a User of Company´s services is involved in money laundering or terror financing, it is their responsibility to report such person to the AML-Co. In such a case, the company must

a. Take the details of the people involved,
b. Verify the type of transactions,
c. Reason for suspicion,
d. The amount involved.

The company must consult with the legal department before embarking on business with a third party and carefully screen such interactions.

4.4. The AML-Co. will carry out the procedure to identify any irregularity on behalf of any stakeholder under this Program. The Company should:

a. Identify all the financers of the company and verify their identity,
b. Take special care where stakeholders want anonymity,
c. Maintain proper records of the stakeholders.

4.5. The AML-Co. should play an active role in the identification and reporting of suspicious transactions. Principal functions include:

a. Reviewing all internal reports from Employers, Individuals and, in light of all available relevant information, determining whether or not it is necessary to make a report to the relevant Financial Intelligence Unit.

b. Maintaining all records related to such internal reviews.

c. Providing guidance and training to all personnel on how to spot suspicious transaction, how to avoid „tipping off" if any disclosure is made.

d. Acting as the main point of contact with the relevant Financial Intelligence Unit and any other competent authorities in relation to ML/TF issues.

5. Prohibition of cash transactions

5.1. Monetary transactions in cash (handover and receipt of cash) in a value greater than or equal to USD 5,000 are not permitted. It is also permitted to transact in cash in value denominated in different currency than USD representing value of USD 5,000 after conversion.

5.2. A safe monetary transaction can consist of one transaction, but also of several individual transactions, if there may be a connection between them.

5.3. If the relevant national legislation sets a lower threshold value in the form of reliefs or prohibitions regarding cash transactions, these take precedence.

6. Documentation and storage

6.1. Relevant national statutory and supervisory requirements for documentation of measures taken in connection with the fight against money laundering and the resolution of identified money laundering-related problems must be observed in addition to the requirements contained in this Program.

6.2. The same applies to established information obligations towards state authorities according to relevant national legislation. In doing so, internal data protection guidelines as well as applicable national data protection regulations and legal retention periods must be observed.

7. Withdrawal and deposit requirements

7.1. All deposits and withdrawals on User´s accounts held with Company follows strict requirements:

a. Company cannot receive or deposit funds from/to third parties.

b. Funds send to Company bust be from bank account, Credit/Debit card or Alternative Payment Method held under the same name as User´s account held with the Company.

c. All funds withdrawn from User´s account must go to a bank account, Credit/Debit card or Alternative Payment Method held under the same name as the User´s account held with the Company.

d. All withdrawal requests are processed according to the funding source of origination. For example, a deposit made via Debit/Credit Card; then a subsequent withdrawal request is received. The amount of funds sent back to the relevant Debit/Credit Card, when a withdrawal request is received, may not exceed the original amount deposited from same. Any profits made in excess of the deposited amount will be transferred to a nominated bank account, which must be held in the same name as your User´s account held with the Company.

8. Know your Customer and Due Diligence

8.1. Company is strongly committed to implement and adhere to AML and KYC policies, each client has to undergo a verification procedure. Before Company starts any cooperation with the User, the Company ensures that satisfactory evidence is produced or such other measures that will produce satisfactory evidence of the identity of any User or counterparty are taken.

8.2. The Company applies heightened scrutiny to Users, who are residents of other countries, identified by credible sources as countries, having inadequate AML standards or that may represent a high risk for crime and corruption and to beneficial owners who resides in and whose funds are sourced from high risk countries.

8.3. In case of Individual User following documents might be required in order to verify personal information:

a. Current valid passport (showing the first page of the local or international passport, where the photo and the signature are clearly visible); or

b. Driving licence which bears a photograph; or

c. National identity card (showing both front and back pages);

d. Documents proving current permanent address (such as utility bills, bank statements, etc.) containing the client's full name and place of residence. These documents should not be older than 3 months from the date of filing.

8.4. In case of Business entity following documents might be required in order to verify KYC information:

a. Certificate of incorporation;

b. Memorandum of Association;

c. Statutes;

d. Social contract;

e. The entity´s decision from on the appointment of a representative who is authorized to access the account held with the Company;

f. The company's decision to open an account. In case the registered owner acts as a representative of the ultimate owners, it is necessary to:

- A copy of the contract and representation;

- POI and POR of the following persons:

  - a representative who is authorized to access the account;

  - final owners;

  - a representative of the owners.

8.5. The Company reserves the right to refuse to transfer or receive funds from third parties representing higher than average risk of AML and TF. The Company also reserves the right to postpone transactions with PEP´s, including withdrawals.