Pursuant to the Statute of Limit Markets Ltd., Port Vila, Vanuatu, and in accordance with the Anti-Money Laundering & Counter-Terrorism Financing (AML&CTF) Act No. 13 of 2014 and the amendments according to the AML & CTF Act No. 16 of 2017, as were published in the Official Gazette No. 45 of 2017, dated 16th of June 2017, the Board of Directors of Limit Markets Ltd., at its session held on 27.09.2017. has adopted the:

PROGRAM FOR RISK ANALYSIS OF MONEY LAUNDERING AND TERRORISM FINANCING

Policy Version 1.1

The content:

INTRODUCTION

The Guidelines of the Securities Commission point to the uniform application of the provisions of the Law on Prevention of Money Laundering and Terrorism Financing, and the regulations adopted pursuant thereto, to those subject to the supervision of the Securities Market.

This Anti-Money Laundering and Terrorist Financing Risk Analysis Program contains: a reference to the importance of the prevention of money laundering and terrorist financing and the definition of the two terms; a way of identifying business opportunities with a client; customer risk assessment; how to determine the riskiness of products and services, from the aspect of anti-money laundering and terrorist financing; a way of identifying a client; preventing the use of new technologies for the purpose of money laundering or terrorist financing; managing the risks of money laundering and terrorist financing to which taxpayers are exposed; employee training program; record keeping, protection and storage of data, authorized persons, and their responsibilities.

In order to apply risk assessment to anti-money laundering and terrorist financing (PN / FT) requirements, this Program shall first identify the risks of money laundering and terrorist financing related to the Company's operations, in the manner in which they are identified and assessed. The possible risks, and the risk assessment itself is the first step to be taken, before establishing and developing PN / FT control and prevention measures to ensure that the measures are appropriate to the nature and size of the Company's business.

THE IMPORTANCE OF PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

Money laundering and terrorist financing are global issues that can have a negative impact on the economic, political, security and social fabric of the country. The consequences of money laundering and terrorist financing threaten the stability, transparency and efficiency of the country's financial system, cause economic disruption and instability, threaten reform programs, reduce investment, harm the country's reputation and threaten national security.

PN / FT risks also arise from a failure to implement the Law on the Prevention of Money Laundering and Terrorism Financing and the related by-laws. Due to the failure to prevent the risk of money laundering and terrorist financing, a taxpayer may be significantly exposed to the risk of compromising his own reputation and the risk of imposing penalties on him by the regulatory authority.

DEFINITION OF MONEY LAUNDERING AND TERRORISM FINANCING

The law on the prevention of money laundering and terrorist financing means the following terms:

Money laundering

Money laundering within the meaning of this Law shall be considered in particular:

▪ replacing or transferring money or other property with the knowledge that they originate from, or have been involved in, criminal activities, with a goal of concealing or fraudulently displaying the unlawful origin of property or assisting a person involved in the commission of criminal activities to avoid sanctioning his conduct;

▪ concealment or misrepresentation of the nature, origin, location, movement, disposition or property of money or other property with the knowledge that they originate from or have been involved in a criminal act;

▪ the acquisition, possession or use of property with the knowledge that at the time of receipt the property originates from a crime or involvement in the act;

▪ participation in the execution, association for the purpose of execution, attempted execution and assistance, encouragement, facilitation and counseling in connection with the execution of the actions referred to in subparagraph 1. 1, 2 and 3 of this paragraph.

Money laundering shall also be considered the acts referred to in paragraph 1 of this Article carried out in the territory of another state.

Financing terrorism

The financing of terrorism, within the meaning of this Law, is considered in particular:

▪ securing or raising, or attempting to secure or raise money, securities, other assets or property, in any way, directly or indirectly, with the intention of using them or knowing that they will be used, in whole or in part, for enforcement of a terrorist act;

▪ encouraging or assisting in securing or raising funds or property referred to in item 1 of this Article.

RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORISM FINANCING

Each institution, regardless of its size and complexity, is required to develop an appropriate system for managing the risk of money laundering and terrorist financing. This risk management system should

ensure that all PN / FT risks are continuously, comprehensively identified, evaluated, monitored, mitigated and managed.

The Company is required to perform a risk analysis that determines the risk assessment of the customer or individual client groups, business relationships, transactions or products in order to prevent the use of its services or products for the purpose of money laundering or terrorist financing.

RISK ANALYSIS CONTENT

Risk analysis consists of the following elements:
- Client identification
- Determining client eligibility
- Risk assessment of individual client, client group and business relationship
- Determination of risk of products and services, from the aspect of prevention of money laundering and terrorist financing
- Defining client risk categories
- Monitoring client accounts and transactions
- Managing the risks to which the Company is exposed in the field of anti-money laundering and terrorist financing
- Professional training and improvement of employees of the Company
- Authorized person for the prevention of money laundering and terrorist financing
- List of indicators of suspicious transactions in the capital market

Client identification

Before establishing a business relationship, it is mandatory to identify the client, which includes:

▪ Identification of the client's identity, that is, if the identity has been previously established, identity verification based on credible, independent and objective sources;

▪ collecting customer data, that is, if data is collected, verifying the data collected through credible, independent and objective sources.

➢ Identifying and verifying the identity of an individual or entrepreneur

An employee of the Company establishing a business relationship with a client determines and verifies the identity of the client who is a natural person, that is, their legal representative, entrepreneur, or a natural person who carries out the activity, by inspection of the client's personal document issued by the competent state body (based on which one can undoubtedly establish his identity) with his presence and obtain the following information:

▪ first and last name, date and place of birth, place of residence,

▪ the number of the identification document and the place of issue, the type and name of the authority that issued the identification document and the unique identification number of the natural person who opens the account, establishes a business relationship or conducts a transaction;

▪ first and last name, date and place of birth, place of residence, number of identification document and place of issue, unique identification number of a proxy who opens an account for another person, establishes a business relationship or conducts a transaction;

▪ date of opening an account or establishing a business relationship;

▪ the type and purpose of the transaction;

▪ date and time of the transaction; transaction amount; ▪

the way the transaction is performed.

➢ Identifying and verifying the identity of a legal entity

An employee of the Company establishing a business relationship with a client establishes and verifies the identity of the client, who is a legal entity, that is, their legal representative, or an authorized person, by seeing the original or certified copy of the document (which must not be more than three months old) or other appropriate public register, filed on behalf of a legal entity by a legal representative.

Identifying and verifying the identity of a legal entity and obtaining the information referred to in Article 71, item 1 of the Law may also be performed by accessing the appropriate public register. In this case the date, time and personal name of the person who carried out the inspection shall be indicated on the

excerpt from the register to which the inspection was made. The excerpt from the registry is stored in a file with other client documentation.

If by inspecting the originals or certified copies of the documents it is not possible to ascertain the particular information prescribed by the Law, the missing data shall be obtained directly from the representative or authorized person.

If an employee who establishes and verifies the identity of a legal entity doubts the authenticity of the information obtained or the authenticity of the documents and other business documents from which the information was taken, he or she must obtain a written statement from the agent or authorized person before establishing a business relationship or executing the transaction.

If a party is a foreign legal entity that conducts business in Vanuatu through its business unit, it is mandatory to identify and verify the identity of the foreign legal entity and its business unit.

Identification of the client - legal entity includes:

▪ the company, headquarters, address, identification number, tax identification number (hereinafter: PIB) of the legal entity that opens an account, establishes a business relationship or conducts a transaction, or for which an account is opened, establishes a business relationship or conducts a transaction;

▪ date of opening an account or establishing a business relationship;

▪ the type and purpose of the transaction;

▪ date and time of the transaction;

▪ transaction amount;

▪ the way the transaction is performed.

In identifying the client, the following actions are also taken:

▪ prior to establishing a business relationship or conducting a transaction, the identity of the client as well as the identity of the real owner are determined and verified on the basis of documents, data and information that can be used to establish the identity in an undoubted and reliable manner;

▪ measures are taken to enable verification and determination of the client's ownership structure and actual control over the client in order to determine the identity of the client's real owner;

▪ data and documentation are obtained and stored on the basis of which the identity and risk factors of the client are determined;

▪ the business relationship with the client is constantly monitored, including transactions during that relationship (whether the transactions correspond to the type of business and client's risk and information about that client), the records are kept and records of business relationship are monitored;

▪ If possible, before establishing a business cooperation with the client, reasons are identified as to why the client has terminated its contractual relations with another participant in the securities market;

▪ When conducting transactions of a customer that is identified, using technologies that do not involve direct contact, procedures are followed to allow the prior verification of the authenticity and accuracy of the transaction order and the authenticity of their submitter.

Identification of the representative or authorized person

When establishing a business relationship or undertaking a transaction by an agent or authorized person (proxy), identification is made of the authorized person (representative, proxy) and the client on whose behalf and for whose account the transaction is opened or performed, solely on the basis of personal or other public documents, namely:

▪ documents issued in the prescribed form by a state body within the limits of its jurisdiction, that is, institutions and other legal entity within the framework of legally entrusted public authorization and written authorization - a power of attorney certified by a notary, consulate, court or state administration body.

If, when determining and verifying the identity of a representative, the accuracy of the information obtained is suspected, especially in cases where:

▪ a written authorization (power of attorney) given to a person who clearly does not have a close enough relationship (eg. relatives, business, etc.) with the client to carry out transactions using the client's account;

▪ when the client's financial status is known and the funds in or in connection with the client's account do not correspond to his or her financial status;

▪ when some unusual transactions are noticed during the business relationship with the client, a written statement is also required.

Identifying the beneficial owner of the legal entity

As part of the verification and review of a client who is a legal entity, in addition to identification, the actual owner of that legal entity is identified by implementing measures in order to obtain data for the natural person who is the actual owner.

In the case of a high-risk client, confirmation of the information obtained is obligatory, if it was not obtained from a confidential and independent source (e.g. if the sole source of the information in determining the client's identity was a written statement of the legal representative, in which case the data up to the extent to which the ownership of the legal entity and the structure of its control are understood, in order to identify all the beneficial owners of the client).

The actual owner of a company or legal entity within the meaning of the AML&CTF Act shall be considered:

▪ a natural person who, directly or indirectly, holds at least 25% of the business interest in shares, voting rights or other rights, on the basis of which he participates in the management, that is, participates in the capital with more than 25% stake or has decisive influence in the management of the assets of the company , that is, a legal entity;

▪ a natural person who indirectly provides or secures funds to a company or legal entity, and on that basis has the right to make a decisive influence on the decision-making of the company management body or legal entity when deciding on financing and operations.

The real owner of a foreign law person (trust, fund or the like) who receives, manages or distributes property for specific purposes, for the purposes of this Law, shall be considered:

▪ a natural person who, directly or indirectly, owns at least 25% of the assets of a legal person or similar entity of foreign law;

▪ a natural person who is designated or determinable as a beneficiary of at least 25% of the income from the assets being managed.

Ownership data are obtained on the basis of the original or a certified copy of the extract from the court register or other official registers submitted by the legal representative or authorized person on behalf of the legal entity, as well as by direct verification in the court register or other public register, or through other available sources.

If all statutory information relating to the beneficial owner (e.g. date and place of birth) cannot be obtained from the court registry or other official register, the missing information is obtained from the legal representative or his authorized representative.

When establishing a business relationship, the client is advised of the obligation to provide written notice of any change related to the beneficial owners.

➢ How to determine client eligibility

After completing the process of identification of the client and the real owner, if the client is a legal entity, information is obtained on the purpose and nature of the business relationship or transaction and other data in accordance with the Law on Financial Supervision, the client's eligibility is evaluated on the basis

of obtained and verified data and information about the client before establishing a business relationship. The assessment of the client's eligibility is usually performed by an employee of the Company establishing the business relationship. In the event that there are indications of increased risk, the employee shall consult with an AML & CFT authorized representative and / or his deputy.

When identification, i.e. acquisition and verification of all statutory client information is performed, the Company establishes a business relationship with the client.

In certain cases, the Company refuses to establish a business relationship with a client, or terminates an already established relationship (if current clients are involved). Such decision shall be taken by the Executive Director or the person designated by him, upon the proposal of the AML & CFT authorized person and / or his deputy.

We decline to enter into a business relationship with the following clients:

▪ If the country of origin of the client or the real owner of the client is on the list of non-cooperative countries, issued by the FATF Working Group on Financial Measures, or on the list of countries considered by the supervisory authority to be risky based on its own off-shore Fig.);

▪ If the client is the person or the actual owner of the client is a person from the country where the measures were implemented under the UN Security Council Resolutions;

▪ If the client is a person on the List drawn up under UN Security Council Resolutions;

▪ If the client is on the Company's internal list, which is formed on the basis of data obtained in communication with the Directorate for the Prevention of Money Laundering and Terrorist Financing;

▪ If, despite taking all the necessary steps to identify them, the identity of the actual client is more seriously suspected

RISK FACTORS

The risk factors on the basis of which the Company, as a participant in the capital market, determines the degree of client's riskiness, business relationship and transactions are:

Geographic risk

Client risk

Transaction risk

Service risk

Geographic Risk

Increased risk of money laundering and terrorist financing is present with clients from certain destinations, in particular:

▪ States subject to sanctions, embargoes or similar UN measures;

▪ Countries designated by the Working Group on Financial Measures against Money Laundering - FATF or other reference international organizations, such as those that finance or support terrorist activities, as well as those with specific terrorist organizations operating in them;

▪ Countries designated by the FATF or other reference international organization as countries lacking an internationally recognized standard for the prevention and detection of money laundering and terrorist financing;

▪ Countries designated by the competent international organizations as having a high level of organized crime for: corruption, arms trafficking, slave trade or human rights violations;

▪ Countries which, according to an international organization (FATF, Council of Europe, etc.), are classified as non-cooperative states or territories; ▪ Countries representing off-shore areas.

Client Risk

A client with an increased risk of money laundering and terrorist financing is a client to whom one of the indicators of suspicious transactions in the list provided in the annex to this regulation may relate.

Transaction Risk

A transaction containing an increased risk of money laundering and terrorist financing is any transaction to which any of the indicators of suspicious transactions in the list provided in the annex to this regulation may be linked.

Service Risk

The following categories of services are considered particularly risky:

▪ services that are new to the market; not previously offered in the financial sector and must be monitored separately to determine the true degree of risk;

▪ electronic issuing of securities trading orders;

▪ providing services to persons with whom a business relationship has not been previously established within the meaning of the Act;

▪ providing services by opening joint accounts that mobilize funds from different sources and from different clients, which are deposited into one account opened in one name;

▪ payment of funds to the dedicated accounts, where it is not certain that the service will be provided.

RISK CATEGORIES

Following the verification and review of the client, based on identified risk factors, the client is classified into a specific risk category of money laundering or terrorist financing.

Since the analysis of the risk of money laundering and terrorist financing requires a good knowledge of the client and his business, the classification of clients by risk category is conducted by the employee who knows the client best in cooperation with the Authorized Person for the prevention of money laundering and terrorist financing.

Immediately upon establishing a business relationship, the client's risk profile is determined and the client is classified into a specific risk category.

During the course of the business relationship with the client and the monitoring of his business activities, all data is updated and the client is classified into the appropriate one in the classification category. If individual client transactions are found to deviate significantly from the normal course of business, an additional analysis of the client's business will be conducted to determine the reasons for such deviation. Based on additional analysis, the debtors will evaluate the client's risk profile and possibly reclassify it.

All clients receive one of the following three risk profiles:

This scale is set out in the Risk Analysis Guidelines to prevent money laundering and terrorist financing, detailing what each category entails. The items on each category are sorted in detail.

CUSTOMER RISK ASSESSMENT

- Normal inspection and monitoring

In addition to client identification, customer review and monitoring measures are implemented, especially when:

▪ opening a securities account or establishing another form of business cooperation with a client;

▪ for each transaction or for several interconnected transactions totaling € 15,000 or more;

▪ when there is doubt about the accuracy or credibility of the customer identification information obtained;

▪ any transaction, regardless of the value of that transaction, if it is suspected of money laundering and terrorist financing related to the transaction or the client.

Client review and monitoring measures are:

▪ identification of the client and the real owner, if the client is a legal entity;

▪ obtaining and verifying information about the client, that is, the real owner, if the client is a legal entity, obtaining information about the purpose and nature of the business relationship or transaction, and

▪ after establishing a business relationship, regularly monitor the client's business activity and check the compliance of these activities with the nature of the business relationship and the usual volume and type of business of the client.

In-depth review and follow-up

This form of client verification is performed in the following cases:

▪ if the client is a politically exposed person; ▪

if the client is identified in the absence.

➢ The client is a politically exposed person

The status of politically exposed persons and their immediate family members and close associates is determined in one of the following ways:

▪ by completing a written form by the client; ▪

collecting information from public sources;

▪ collecting information based on insights into databases that include lists of politically exposed persons (e.g. list of politically exposed persons on the Administration's website, World Check PEP List, etc.);

▪ collecting information based on an insight into the records of the Commission for the Prevention of Conflict of Interest.

Identifying close associates of politically exposed persons applies if the relationship with the associate is publicly known.

Before establishing a business relationship with a politically exposed person, the following actions are performed:

▪ data on the source of assets and assets that are the subject of a business relationship or transaction are obtained from personal and other documents submitted by the client, and if the prescribed data cannot be obtained from the submitted documents, the information is obtained directly from a written statement of the client;

▪ The written consent of the CEO is obtained before establishing a business relationship with the client.

Data on politically exposed persons shall be kept in the electronic form.

➢ Identifying the client's identity in the absence

When identifying and verifying the identity of a client who is not present, the following additional measures are also taken:

▪ Supplementary documents, data or information are obtained on the basis of which the identity of the client is verified;

▪ documents submitted are verified or confirmation is obtained from the financial organization performing the payment transaction that the first payment of the client was made at the expense of the account kept with the respective organization.

Simplified review and monitoring

Simplified client verification is done when it comes to:

▪ state bodies, local self-government bodies and other legal entities exercising public authority;

▪ companies whose securities are admitted to trading in EU member states or other countries where EU standards are applied on stock exchanges;

▪ to the persons referred to in Article 4, paragraph 2, item. 1, 2, 4, 5, 6, 8, 9 of the Law, as well as other relevant organizations based in the EU, US or in a country listed by the Ministry of Finance.

CONTROL OF CUSTOMER ACCOUNTS AND TRANSACTIONS

The accounts and transactions of the client are continuously monitored to prevent money laundering and terrorist financing. To this end, information about the client's business is collected and an assessment of the compliance of the transactions with the client's profile is made. Particular attention is paid to all

complex, unusually large transactions and all unusual activities that have no obvious economic or legal purpose. The List of Suspicious Transactions Indicators, which is an integral part of this Rulebook, is used.

Monitor client accounts and transactions, depending on risk category:

- high risk category - at least quarterly

- medium risk category - at least twice a year

- low risk category - at least once a year

BUSINESS RISK ASSESSMENT AND RISK MANAGEMENT

Risk is a function of the likelihood of risk events occurring and their impact. The likelihood of an event is a combination of threats and vulnerabilities, that is to say, risk events occur when the threat exploits the vulnerability. Accordingly, the level of risk can be reduced by reducing threats, vulnerabilities or their impact.

In order to determine the Company's exposure to ML / FT risk and to view the effective management of that risk, the Company must identify each segment of its business in which the ML / FT threat may arise and must assess its vulnerability to that threat. It is imperative that ML / FT risks are continuously identified at all levels of management - from the operational level to the executive board - and that all organizational units of the Company are involved in the process. Most and the complexities of the business play an important role in deciding how attractive or risky ML / FT is. For example, when an organization is large, it is less likely that it will know the client personally, so that client may be significantly more anonymous than the client of a small organization. Likewise, an organization providing services internationally may be more attractive for someone who wants to launder money than a domestic organization would.

Once the risks are identified, the Company adequately assesses the exposure to the risk of money laundering and terrorist financing, which makes it possible to assess the likelihood of a negative impact that could arise from that risk, as well as the potential effect of that risk on the achievement of its business objectives.

Risk identification and analysis are conducted for all existing and new products, activities and processes. An effective ML / FT risk identification and analysis process and risk analysis serve as a basis for establishing an appropriate risk management and risk control system and, consequently, for achieving the ultimate goal - minimizing any adverse effects that may result from that risk.

The assessment of the risks of money laundering and terrorist financing assumes that the various services offered by the Company as part of its business are not equally susceptible to misuse. A risk assessment is carried out to make it possible to apply control measures commensurate with the identified risk. This allows the Company to focus on those clients who present the highest potential risk.

In summary, a comprehensive system for assessing and managing the risks of money laundering and terrorist financing involves:

- risk identification;
- measurement and assessment;
- monitoring and analyzing risks;
- controlling and minimizing risks;
- Notifying supervisory authorities.

The risk management system will be established and gradually developed.

Risk assessment is proportionate - Appropriate attention must be paid to the large and significant difference in business practices, size and expertise among taxpayers. There are various forms of risk assessment depending on the size of the Company and the business it performs. The checklist attached in Schedule 1 to this document is appropriate for smaller payers, and is the starting point used by the Company in view of the nature of the scope of the business. It provides an example of an initial risk assessment of a customer, product, service, business and geographical area.

PREVENTING THE USE OF NEW TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING

The widely used new technologies that enable anonymity (internet banking, use of its ATMs) for the purpose of fast moving financial resources have further complicated investigations in cases of suspected money laundering or terrorist financing. When performing money transfer services, the Company is obliged to collect the following information about the payer as mandatory:

- Name of the legal entity of the payer, i.e. the name and surname of the individual of the payer
- Head office of the payer's legal entity, i.e. address of the payer's residence or residence and physical person (this information may be replaced by: date and place of birth of the payer's natural person, payer's identification number and unique identification number of the payer: legal entity's identification number or personal identification number or PIN number of the physical persons engaged in economic activities, or PIN numbers of natural persons not engaged in economic activities).

▪ Account number (if the payer does not have an account, the Bank replaces the account number with an identifier that allows monitoring of the transfer from the payer.

The Company determines whether all information about the payer has been entered in the form or the message accompanying the electronic and the transfer of funds. When the Company determines that the absence of accurate or complete information on the payer is a basis for suspicion of money laundering or terrorist financing, it shall immediately inform the competent authority.

Identification

Prior to the transfer of funds, the Company is obliged to establish and verify the identity of the payer by examining the payer's identity documents issued by the competent authority.

In the case of transfer of funds from the account, identification of the payer is considered to have been made if:

▪ verification of the identity of the payer was done during the account opening;

▪ for the payer with whom the Company has already established a business relationship (old client), subsequently conducts a check or obtains data in accordance with the Law on AML&CFT

The company establishes and verifies the identity of the payer in each case, regardless of the amount and type of transaction when there are reasons to suspect that it is money laundering and terrorist financing and notifies the authorized person without delay.

PROFESSIONAL TRAINING AND TRAINING

In accordance with the legal obligation, the Company takes care of the professional training and training of its employees for the purpose of preventing and detecting ML / FT. Vocational training and training of employees involves, first of all, acquaintance with the provisions of the Act and by-laws adopted by the law, with the internal act of the taxpayer, with international standards arising from international conventions in the field of AML&CFT, and with guidelines and a list of indicators for identification of suspicious transactions, as well as obligations to notify the competent authorities and keep records. The professional training and training of employees related to the prevention of money laundering and terrorist financing aims at raising the awareness of employees about the importance of timely measures taken to prevent money laundering and terrorist financing.

The Company has established a system of vocational training and training to keep abreast of news, including current techniques, methods and trends in the field of AML&CFT, and provides clear explanations of all aspects of the Law and Obligations regarding AML&CFT, and in particular the requirements that are related to customer due diligence, and notification of suspicious transactions.

Employee training related to the prevention of money laundering and terrorist financing includes a good understanding of the regulatory requirements (Laws and By-Laws) and internal policies and procedures adopted by the Company to successfully manage risks in this area.

The timing of the trainings is adapted to the real needs of the field of activity of the employees, in order to be timely and in line with the latest legal acts. The authorized person decides on the need for training, whether it is a newly employed person, an employee who has direct contact with clients or an employee who works with new clients.

The vocational training plan and program are proposed by an authorized person and submitted to the Board of Directors for approval. The authorized person makes a record of the professional training of the employees, which contains the date and place of the training, the names of the persons present during the training and the topic of the training.

RECORDING AND DELIVERY OF DATA

Records all persons and transactions are kept, which includes data and documentation related to the opening of an account, the establishment of business cooperation, as well as the performed transaction. This information and documentation shall be kept in writing and electronically for ten years from the date of the transaction or completion of the business cooperation.

Information on transactions suspected of money laundering or terrorist financing shall be submitted without delay by the Authorized Person to the Directorate for the Prevention of Money Laundering and Terrorist Financing.

DATA PROTECTION AND STORAGE

Employees of the Company, party or third party must not disclose data, information or documentation on the client or transaction it is conducting as it will be disclosed to the Directorate for the Prevention of Money Laundering and Terrorist Financing or that the Administration has temporarily suspended the execution of the transaction or given an order for continuous account monitoring. Requested information,

submission of information, information or documentation and suspension of the transaction and continuous monitoring of the account are an official secret.

The requests of the Administration for the submission of data, as well as the responses to them, are recorded and kept by a special procedure and are marked with the confidentiality provided by the Administration at the request, while the data on suspicious transactions is marked with confidentiality. A special book is opened for the safekeeping of these documents, and kept in a specially protected cabinet, separate from other documentation. Data submitted to the Administration in electronic form is copied and electronic records are also stored in the same mode.

The data and documentation obtained under the Anti-Money Laundering Act are kept for 10 years after the transaction has been completed, the account closed or the contract expires.

The data and documentation on the authorized person and the deputy authorized person, professional training of employees and implementation of internal control in relation to the Law shall be kept for four years after the appointment of the authorized person and the deputy authorized person who has completed professional training and internal control.

The previous information is stored in the same way as the client and transaction documentation provided to the Management Board.

APPOINTMENT OF AUTHORIZED PERSONS

The Anti-Money Laundering & Counter-Terrorism Financing (AML&CTF) Act defines the obligation to appoint an authorized person who is responsible for the implementation of measures and tasks under the Law and related by-laws. Pursuant to this obligation, the Company appointed an authorized person and its deputy and informed the competent authorities accordingly.

Furthermore, the Company has provided appropriate conditions for an authorized person to perform their tasks, such as:

▪ take care of the establishment, operation and development of systems for detecting and preventing money laundering and terrorist financing;

▪ take care of the proper and timely submission of information to the Directorate for the Prevention of Money Laundering and Terrorist Financing;

▪ initiate and participate in the drafting and modification of operational procedures and preparation of the Company's internal acts relating to the prevention and detection of money laundering and terrorist financing;

▪ cooperate in the development of guidelines for conducting checks related to the prevention and detection of money laundering and terrorist financing;

▪ monitor and coordinate the Company's activities in the area of detecting and preventing money laundering and terrorist financing;

▪ cooperate in the establishment and development of information technology to carry out the activities of detecting and preventing money laundering and terrorist financing;

▪ provide the Board of Directors and the Executive Director with initiatives and proposals to improve the detection and prevention of money laundering and terrorist financing systems;

▪ prepare professional training and employee training programs related to the detection and prevention of money laundering and terrorist financing;

▪ prepare and report to the Board of Directors once a year, and more often if necessary.

Also, an authorized person is employed in a workplace that is systematized in the organizational structure of the Company so as to enable the person to perform tasks quickly, accurately and timely. The authorized person is independent in work, appropriately and professionally qualified to carry out the tasks and is well versed in the nature of the Company's operations and exposure to ML / FT risk, and has the ability to communicate directly with the competent authorities.

RESPONSIBILITY

The following are specifically responsible for the implementation of this program:

Authorized person and his / her deputy, in particular for:

▪ timely and accurate submission of reports to the Directorate for the Prevention of Money Laundering and Terrorist Financing concerning suspicious transactions and responses to requests from the Directorate for supplementary data, information and documentation,

▪ transfer of suspension of transactions,

▪ transfer of accounts for continuous monitoring of accounts,

▪ organizing quality employee training,

▪ delivering timely and quality information to the competent bodies of the Company,

▪ updating the list of indicators of suspicious transactions,

▪ innovating programs and procedures in accordance with changes in legislation and needs identified in the implementation process;

▪ adequate data storage.

Direct executors, especially for:

▪ Client identification and transaction

▪ monitoring of client's business activities and application of indicators of suspicious clients and transactions,

▪ timely informing the Chief Executive Officer and the Authorized Person for AML and CFT about the suspected client and / or transaction,

▪ Execution of a temporary suspension order,

▪ Execution of a continuous account monitoring order,

▪ keeping confidential information about a suspicious client and a transaction,

▪ temporarily suspending a transaction and continuously monitoring accounts.

REPORTING

The authorized person is obliged to submit a report on the activities on prevention of money laundering and terrorist financing to the Board of Directors of the Company once a year, and, if necessary, more frequently.

The report should contain, in particular, information on:

▪ the total number of suspicious transaction reports submitted;

▪ the total number of suspicious transactions analyzed by the Company's employees and not notified to the Management Board on the basis of a review and evaluation by the Authorized Person;

▪ the total number of suspended transactions;

▪ the total number of accounts for continuous monitoring of client accounts;

▪ newly discovered ways and techniques of money laundering with proposed measures for their identification and detection;

▪ activities undertaken to resolve problems identified in the application of procedures and practices for identifying suspicious transactions;

▪ the results of the training of employees with information on the date of training, topics covered and the names of the persons who attended the training;

▪ proposing measures to improve policies and procedures for detecting and preventing suspicious transactions.

Once approved by the Board of Directors, the report is submitted to the Directorate for the Prevention of Money Laundering and Terrorist Financing.

THE ENTRY INTO FORCE

This Program is effective starting 27.09.2019.

Annex 1

The checklist is appropriate for smaller payers, and is the starting point used by the Company for reviewing the nature and scope of the business. It provides an example of an initial risk assessment of a customer, product, service, business and geographical area.

Customer risk:

RISK OF THE PARTY		
Does the Company have parties...		
engaged in cash intensive business?	YES	NO
who reside outside Vanuatu?	YES	NO
who are the intermediaries or persons who carry on professional activities and who hold accounts for clients whose identity of the beneficial owners is not established?	YES	NO

which are unregistered charities or other unregulated "nonprofit" organizations (especially those operating on a "cross-border" basis)	YES	NO
which are resident in an area known for its high crime rate?	YES	NO
which offer online gambling?	YES	NO
whose nature of business makes it difficult to identify the actual owners?	YES	NO
whose parties are politically exposed?	YES	NO
that do not have an address or have several addresses for no good reason?	YES	NO

who are known to be involved in criminal activity?	YES	NO
who are connected to organized crime?	YES	NO
PRODUCT / SERVICE RISK		
Does the Company offer products or services which…		
make it difficult to fully identify the parties?	YES	NO
help set up businesses?	YES	NO
lend the address to foreign legal entities?	YES	NO

are in business of concealing the actual owner of the party?	YES	NO
perform real estate transfers between the parties for an unusually short period of time for no apparent legal, economic or other justified reason?	YES	NO
are the provision of services related to the establishment, operation or management of inactive fictitious and nominal companies?	YES	NO
BUSINESS RISK:		
Does the Company perform…		
transactions for which you identify and verify identity without the presence of a party and / or establish a business relationship without the presence of a party?	YES	NO

Does the Company have jobs that include…		
complex financial transactions?	YES	NO
payments to / from third parties and cross-border payments?	YES	NO
high-risk real estate transactions?	YES	NO
cash transactions	YES	NO
GEOGRAPHICAL RISK:		
Does the Company operate or conduct activities in a:		
non-EU country or signatory to the EEA Agreement?	YES	NO

country against which the UN has imposed sanctions, embargoes or similar measures?	YES	NO
country known as a tax haven or financial offshore center?	YES	NO
country identified by the FATF as uncooperative in the fight against money laundering or terrorist financing?	YES	NO
country where terrorist activities are supported?	YES	NO
country where appropriate AML & CFT measures are not being implemented in the assessment of the relevant international organizations?	YES	NO
country that is known for a significant degree of corruption or other criminal activity?	YES	NO