1. General provisions

1.1 The current AML policy has been developed in accordance with the applicable legislation of the St.Vincent & the Grenadines, EU regulation and FATFA Money Laundering and Terrorist Financing Prevention ruling.
1.2 The AML policy is a set of internal rules and regulations that is used by the Company in order to check and reveal documentation and information regarding its operation that is under obligatory control, and other operations with money or property that may be in any way connected to money legalization (money laundering) or finance of terrorism, and the provision of such information to the state authorities.

1.3. The AML policy has terms that appears from time to ties and has the meaning of:

Company – LLC VIPTRADE P. O. Box 1574 First Floor, First St.Vincent Bank Ltd Building, James Street, Kingstown St.Vincent & the Grenadines. (Registration Number : 384 LLC 2020)

- **AML** – Anti-Money Laundering legal controls methods that require Company and other regulated parties to prevent, detect, and report money laundering activities.
- **Money laundering** – is the introduction of assets derived from illegal and criminal activities into the legal, financial and business system. Offences are for example, forgery of money, extortion, robbery, drug crime, prostitution, fraud, corruption, organised crime, or terrorism. Predicate offences for money laundering are defined by local law. The money laundering process consists of three stages:
- Placement: – Introducing illegally obtained monies or other valuables into financial or non-financial institutions;
- Layering: – Separating the proceeds of criminal activity from their source using layers; and
- Integration: – Placing the laundered proceeds back into the economy in such a way that they reenter the financial system as legitimate funds.
- **MLRO –** Money Laundering Reporting Officer – nominated officer appointed under Regulation in force and FATF recommendations which provides oversight for Company's AML systems.
- **AMLTF –** Anti-Money Laundering Task Force of the EBA, ESMA and EIOPA.
- **AML Committee –** The Joint Committee of the European Supervisory Authorities- Sub Committee on Anti-Money Laundering.
- **CTF –** Counter-Terrorist Financing are set of legal and managers decisive actions recommended and undertaken by individuals and staff members in order to impede, straggle with and rededicate results of capitalizing, rendering support and endow/revenue actions of terrorism as defined by UN Convention for the Suppression of the Financing of Terrorism (1999), UN Security Council resolution 1373 (2001), United Nations GA resolution 1267 (1999) and its successor resolutions, the FATF recommendations adopted by the FATF plenary in February 2012 (Updated June 2019).
- **Actions of terrorism** – any act intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act.
- **RBA** – risk-based approach – combination of the likelihood of an adverse event (hazard, harm) occurring, and of the potential magnitude of the damage caused implemented to business process assessments as a quantitative methodology that will not eliminate the risk; however, it will enable the understanding of risks with the aim of mitigating the impact which requires

identification of risk factors, classification and scoring in accordance with FATF 40 Recommendations, 2012.

- **CDD** – customer due diligence – as defined by Sanctions and Anti-Money Laundering Act 2018 is perceived as information comprises the facts about a customer that should enable an organisation to assess the extent to which the customer exposes it to a range of risks through know their customer's procedures with the aim:
- to comply with the requirements of relevant legislation and regulation
- to help the firm, at the time the due diligence is carried out, to be reasonably certain that the customers are who they say they are, and that it is appropriate
- to provide them with the products or services requested
- to guard against fraud, including impersonation and identity fraud
- to help the organisation to identify, during the course of a continuing relationship, what is unusual and to enable the unusual to be examined;
- if unusual events do not have a commercial or otherwise straightforward rationale they may involve money laundering, fraud, or handling criminal or terrorist property
- to enable the organisation to assist law enforcement, by providing available
- information on customers being investigated following the making of a suspicion report/
- **FATF** – the Financial Action Task Force (on Money Laundering) an intergovernmental organization founded to develop policies to combat money laundering and terrorism financing.
- **FATF Recommendations –** set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.
- **EEA –** European Economic Area.
- **EDD –** Enhanced Due Diligence.
- **International sanctions –** are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organizations against states or organizations either to protect national security interests, or to protect international law, and defend against threats to international peace and security.
- **MS –** Member State of the European Union.
- **MVTS –** money or value transfer services – financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer or any other way.
- **PEP –** Politically Exposed Person – individuals having relation to state power institution or being under the interest of state power institution:
- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, of constitutional courts or of any judicial body the
- decisions of which are not subject to further appeal except in exceptional
- circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned
- enterprises;
- directors, deputy directors and members of the board or equivalent function of an
- international organisation;
- individuals under political international sanctions.

- **SARs –** Suspicious Activity Reports – is a document that MLRO must file to regulator, financial institutions and Company's management with the following a suspected incident of money laundering or fraud.
- **SDD –** Simplified Due Diligence.
- **3rd MLD –** Third Money Laundering Directive (2005/60/EC)

1.3 The AML policy is a document that:

1.3.1 Regulates the organization of activity regarding the prevention of legalization of illegally obtained funds (money laundering) and the financing of terrorism;

1.3.2 Sets the obligations and obligatory procedures for the employees regarding internal control;

1.3.3 Sets the terms for the fulfilment of obligations by the employees and sets the authorized control persons.

1.4 The AML policy contains further programs:

1.4.1 A program for the overview of internal control methods;

1.4.2 A program for the implementation of internal control methods;

1.4.3 Client and persons associated with client's identification program;

1.4.4 A risk analysis program;

1.4.5 A program for the regulation of commercial relations with clients;

1.4.6 A program for the regulation obligatory actions in case there are suspicions of money laundering;

1.4.7 A correspondence exchange program;

1.4.8 An information documentation program;

1.4.9 A transaction refusal program;

1.4.10 An employee preparation program;

1.4.11 An internal control program;

1.4.12 A document maintenance program regarding documentation that was obtained during the execution of the internal control program.

1.5 The company is providing financial industries services as investment services, advising services and asset management services.

1.6 The person responsible for the accurate implementation of the present policy is named by the company management board in accordance with the articles of association and applicable legislation.

2. Organizational basis for the control methods

2.1 The person responsible for the implementation of the provisions in the present document is appointed by the written order of the management board of the company.

2.2 In order to adequately implement the current policy, considering the volume of clients and associated risk levels, the company has formed a separate group, including a member of the board, the head accountant and the head of the legal department.

2.3 All subsidiaries and structural parts are accountable before the authorized group in the field of suspicious transactions. All matters regarding initial client identification are handled by the corresponding structural parts of the company.

2.4 Company shall apply FATF Recommendations in force and amend relevant policies from time to time to improve Control (CDD and RBA) mythology within the Company.

2.5 A company official is named as the contact person between Company and the financial institution's MLRO. The contact person must have the required knowledge and skills to carry out his obligation and the present policy. The contact person shall only be accountable before a member of the board and will perform the following tasks as to:

- Design, amend and implement controls to manage and mitigate risks;
- Make analysis of the performed or planned transaction regarding their possible connection to money laundering or finance of terrorism;
- Presentation to the financial inspection of any data regarding clients, their associated persons, and transactions, which may be connected to illegal activity;
- Presentation of reports regarding the fulfilment of this policy;
- Define focal point for all activities within the company relating to AML and CTF;
- Provide AML training to Company's staff
- receiving all internal suspicious activity reports and, where deemed applicable, reporting to relevant authorities on the same
- Establish the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice;
- Support and co-ordinate senior management due anti-money laundering/terrorist financing risk in individual business areas;
- Advise senior management on AML perspective in new products / processes projects;
- Fulfilment of other obligations as set out in the "Money Laundering and Terrorist Financing Prevention Act".

2.6. The Company shall guaranty that the MLRO has sufficient functional and hierarchic independence within the Company, has the adequate experience and constantly updating understanding of AML/CTF to execute his/her functions. The Company shall provide enough resources to MLRO to cope his/her functions and shall define further MLR's development.

2.7 The MLRO, with the support of the senior management, is responsible for ensuring that the Company meets its AML compliance requirements in accordance with applicable legislation. The MLRO will monitor asses and make recommendation to improve the AML systems and controls methods.

2.8 The MLRO is also required to produce reports for senior management, in order to provide control and results of his activity, as due to the following items:

- Confirmation that adequate customer due diligence information is being collected and that ongoing monitoring is taking place;
- Summary data relating to complex or unusual transactions;
- Number of internal consents / Suspicious Activity Reports (SARs) received from staff members;
- Number of SARs sent externally;
- Information on status of staff training within the company;
- Confirmation that all business records have been properly stored and are retained according to regulatory requirements;
- Changes in the law/operating environment which do or might impact the business;
- Changes in the risk matrix affecting the business; and
- Contacts with the regulator.

3. Implementation of control methods

3.1 Control methods are used in the following areas:

- during the initiation of a commercial relationship with the client and during their activity;
- in any case when the sum of the transaction exceeds 1000 EUR or an equivalent in any other currency;
- carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances if:
- wire within Financial institutions (for occasional customers under Recommendation 5) – USD/EUR 15,000.
- wire within Casinos, including internet casinos (under Recommendation 12) – USD/EUR 3000.
- wire within dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) – USD/EUR 15,000
- wire within POA for Lawyers, notaries, other independent legal professionals and accountants in any jurisdiction when, on behalf of or for a client, they engage in a financial transaction in relation to the activities hereabouve;
- if there is any doubt that the provided data is accurate;
- if the planned transaction is needlessly complex;
- if there is any reason to suspect that the transaction is connected with money laundering or finance of terrorism or any other form of illegal activity or is considered a high-risk transaction in accordance with the risk evaluation procedure set out in the current policy.

3.2 Additional control methods are implemented in the event that the Client changes the conditions of the transaction, increasing the risk level:

- If the transaction serves no rational purpose;

- If the transaction is financially irrational;
- If the same type of transaction is repeated multiple times over a short period;
- Should the client refuse to provide information without giving a reason for the refusal or should the client express unusual concern with the matters of confidentiality;
- Should the Client decide to alter the transaction in a manner that is not the usual practice of the organization;
- Should the client express unreasonable hurry to carry out the transaction;
- Should the client implement changes into the transaction conditions shortly before it is performed;
- Should the client prove impossible to contact;
- Should there be any information that the data provided by the client is false or inaccurate;
- In case of absence of any association between the activities of the Client and the planned transaction;
- Should the planned transaction be needlessly complicated and lacking any legal purpose.

3.3 Additional methods for the control of a suspicious transaction:

- Receipt from the client with the necessary explanation and confirmation that clarify the purpose of the transaction;
- Implementation of increased monitoring in accordance with the present policy regarding all the transactions of the Client in order to confirm if they are in any way connected to money laundering or the finance of terrorism.

3.4 Company will guaranty the Client identification and monitoring of transaction as stated by FATFA recommendation.

3.5 The risk-based approach implemented by the Company shall take the most cost effective and proportionate way to manage and mitigate money laundering and terrorist financing risks. It is based under:

- Customer risk – specific categories of customers and the resulting business relationships
- Payment risk – payment methods offered and the degree to which their specific characteristics are vulnerable to ML/TF threats
- Geographical risk – the risks posed by geographical factors
- Product risk – products offered and the degree to which their specific characteristics may be attractive for money laundering or financing terrorism
- Supplier / 3rd party Risk -risks of onboarding new clients / suppliers and not understanding who owns the business or considering other AML risks
- Technological Risk – risks with technology used by the company / how susceptible is it to money laundering or terrorist financing.
- Employee risk – the risks posed by employees of the company
- Regulatory Risk – the risks of non-compliance with license and regulatory frameworks and the risk of penalties to the company and individuals.

4. Client and their associated person's due diligence (CDD)

4.1 The initial identification of the client is made based on the provided client identification document.

4.1.1 Regarding the **physical persons** the following is confirmed:

- Name;
- Surname;
- Patronymic (when applicable to national custom);
- Citizenship;
- Date of birth, personal ID number;
- ID document data;
- State authority issuing the document;
- Date of ID being issued and valid date;
- Place of residence;
- Personal tax number (if applicable);
- Occupation;
- Reason for initiated commercial relations;
- Contact information – phone number, email address.
- Source of funds;
- Wealth confirmation;
- Financial experience and business recommendations.

4.1.2 During identification, the documents are checked for accuracy of the information provided and the following is confirmed:

- Whether the identification document is legally valid;
- Is the photo on it accurate;
- Whether the personal ID code corresponds to the client's gender and age
- Whether the residence of person is permanent and on legal basis;
- Whether the occupation, experience, source of wealth and business intentions have common points;
- Whether business interests are assumed, assessed and not out of business spontaneous decision;
- Customer reaction, good business attitude and reputation as contra party adequate behavior.

4.1.3 Should there be any doubt regarding the document, the state authorities/financial institution that issued the document may be contacted in order to obtain the necessary confirmation.

4.1.4 Should the Client present an ID, a copy is made, the quality of which allows reviewing the data contained in the document.

4.1.5 When the identity of a physical person is confirmed it is also confirmed whether he is a state official;

4.1.6 A state official is a person who has a state appointed position in any country of the European Union or any other country or who holds a position in an International organization. Further data regarding the state officials to be gathered:

- List of the closest associates and relatives (if such information is publically available);
- Confirmation of the property and sources of income that are meant to be used in the transaction;
- Preparation of an inquiry to the proper database;
- Preparation of an inquiry to the state supervision institutions;
- A person named in accordance with provision 2.1 of this policy makes a decision regarding the start of the commercial relationship with the state official.

4.1.7 Only official sources may be used to check the provided information, such as state registries or foreign representatives. Other sources may be used if there is no doubt regarding their accuracy and competence.

4.1.8 Trustworthy Client recommendation does not replace the proper review of information.

4.1.9 Identification of a physical person that acts as a representative is made in accordance with the provisions of this policy.

4.1.10 Identification of a physical person is not a one-time procedure. The information regarding the physical person should be checked constantly and updated when necessary.

4.1.11 Should there be any doubt, the actual beneficiary must be revealed – a person that actually controls the legal person and receives profit from it.

4.1.12. The CDD and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17 shall be made to designated non-financial businesses and professions (DNFBPs) acting on third parties interest under POA in cases they are related to any activity within:

– Casinos representatives of beneficiaries engaged in financial transactions equal to or above the applicable designated threshold.

– Real estate agents involved in transactions for their client concerning the buying and selling of real estate.

– Dealers in precious metals and dealers in precious stones engaged in any transaction with a customer equal to or above the applicable designated threshold.

– Lawyers, notaries, investment dealers, other independent legal professionals and accountants carrying out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contributions for the creation, operation or management of
- companies;
- creation, operation or management of legal persons or arrangements, and
- buying and selling of business entities.

– Trust and investment company service providers staff members carrying out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

4.2 The following information must be obtained during the registration of a legal person:

4.2.1 Regarding the **legal persons** the following information is gathered:

- Name of the legal entity;
- Registration number;
- Legal address and the address of principal activity;
- Corporate form;
- Full information regarding legal representatives;
- Beneficiaries;
- Company group structure;
- Company's customers and supplier's geography;
- Company business activity and partners;
- Beneficiary source of wealth;
- Beneficiary corporative investment structure;
- Company good business reputation and court rulings in actions;
- Market risks and forecasts.

4.2.2 The review of information is made by the use of public registries and databases or by sending inquiries to the state authorities. Certificate from a registry may be replaced by an authorised access to the registry.

4.2.3 All documents issued by foreign state authorities must be legalized or have an apostille, except the documents from CIS states (According to Minsk Convention of 1992). The present provision may be amended if [company's country] and their contracting parties jurisdictional authorities signs and ratifies an international agreement with other states that will make the apostille unnecessary.

4.2.4 The control of the legal entity management board or another similar control organ must also be carried out regarding their connection to state officials, also regarding beneficiaries and their representatives. Should the information provided by the Client not be trustworthy enough, the information may be reviewed by the means of an inquiry to state officials or international organizations.

4.2.5 All the provided information is gathered and carefully studied to reveal whether the company has any subsidiaries, representatives or is in any way connected to countries that do not cooperate in the field of international opposition to money laundering and finance of terrorism, or if those states are considered to be low tax jurisdictions.

4.2.6 If the legal entity is an international organization, then its field of activity must be confirmed by the provisions of documentation regarding activities in [company's country]. The information in the documents must be checked.

4.3 If the legal entity acts as a representative of another entity, then the information of that other entity must also be gathered in accordance with this policy.

4.3.1 Only an authorised legal representative may register a legal entity on the website of Company. The authorised representative must provide sufficient documentation proving his authority to represent the legal person. Should the provided documents fail to provide the required information or if there is any doubt regarding their accuracy, no commercial relationship may be initiated and the account may be blocked. The document proving the authority must contain further information:

- Scope of rights;
- Date the authority was granted and for what period;
- Reason the authority was granted.

4.4 Any transaction with the legal person requires the registration of the current beneficiary.

4.4.1 Should a person have more than one beneficiary, then all other beneficiaries must also be registered.

4.4.2 Should it prove impossible to clarify the beneficiaries of the company, all owners of the company must be confirmed and the Client must provide sufficient explanation.

4.4.3 Special care should be taken when confirming the actual beneficiary if the planned transaction may in any way be connected to the increase of the risk due to the field of activity of the legal person, state of registration, type of provided services and nature of the transaction, and also if the legal person is registered or connected to a low tax jurisdiction.

4.5 A non-resident legal person must abide by the same identification process outlined above. Company has the right to deny any transaction if the legal person is a resident of a country whose legislation violates the provisions of this AML policy.

4.6. **Non-profit organizations** shall be AML focused by aim, Staff members, partners and financial Tran's active institution's AML or supervisor.

4.6.1 Company should apply focused and proportionate measures, in line with the risk based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

(a) by terrorist organizations posing as legitimate entities;

(b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

(c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

4.6.2 Within this Company shall identify each founder, senior manager, controller, financial supervisors, financial institution AML related within the transactions and final causa noble aim that shall be shared, reflected and have exclusive connection to all stake holders.

4.6.3. Non-profit organizations shall be recognized and proved by state jurisdiction of registration within the Annual Report (Financial Report) being supplied or publically available.

4.7 **Limited Companies and Limited Liability Partnerships** shall be AML assessed by information due to founding members, final benefiter owners, controlling persons (corporative directors if any) and professional business experience (beneficiary, staff member).

4.7.1. The following documentation is required to identify a Partnership.

Business Account Application signed by a partner;

Photographic ID for all partners – current passport or photo-card driving license;

Current address verification (bank statement or utility bill) of both personal and business addresses, no more than three [3] months old;

Copy of Registration of each partner with the HMRC as self-employed – Self Assessment letter or VAT certificate issued when trading commenced;

Partnership Agreement (if available); and

VAT number if applicable.

4.7.2. The following documentation is required to establish a relationship with a Limited Liability Partnership (LLP).

Business Account Application signed by a Client: Someone who has the authority to bind the partnership;

Copy of LLP certificate registered with Companies House;

Current address verification (bank statement or utility bill) of personal and business addresses, no more than three [3] months old;

VAT number if applicable; and

Identification of at least two designated owners, and identification any further owners who hold a beneficial interest in the company.

4.7.3. The following documentation and identification is required to identify a Limited Company.

Corporate Account Application signed by a Shareholder or Director of the company or any other person who has the authority to bind the company;

Registered office address, registered number and principal place of business;

Board of directors;

Senior persons responsible for its operations;

Identification of at least one Director and identification for any shareholder who holds a beneficial interest in the company of greater than twenty-five [25] percentage.

Certificate of incorporation (if a Client is a foreign company, a certified copy of an equivalent document from a lawyer of the home country);

Current address verification (bank statement or utility bill) of business address, no more than three [3] months old; and

VAT number if applicable.

4.8 **Trusts** shall be AML assessed by information concerning the Settlor, the Trustee(s), the Protector, the Aim and professional experience within the real going business.

4.9 **Sole Trader / Sole Proprietor** shall be identified by:

Business Account Application signed by sole trader;

Photographic ID of sole trader – Current passport or photo- card driving license;

Current address verification (bank statement or utility bill) of business address, generally no more than three [3] months old;

Copy of Registration of sole trader with HMRC as self-employed – Self Assessment letter or VAT certificate issued when trading commenced; and

VAT number if applicable,

4.10 Sanctions and PEPs Screening are both used within the legal entities identification as physical person identification.

4.10.1 The Company shall use open sources service provider to verify clients against declared Sanctions Lists and Politically Exposed Persons (PEPs) lists. Individuals shall be checked on perpetual basis (not less that once per month) as well as on initial registration.

4.10.2 The Company will take all required steps to ensure that all customers with whom a business relationship is established are screened against relevant notices such as:

- the Office of Foreign Assets Control (OFAC)
- European Union sanctions (EU)
- United Nations sanctions (UN)

4.10.3 Any confirmed matches to sanctions lists shall be declined or closed, and the necessary reports will be made to senior officers and financial institutions for transaction.

4.10.4 The company must have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is—

(a) a politically exposed person (a “PEP”), or

(b) a family member or a known close associate of a PEP, and to manage the enhanced risks arising from the relevant person’s relationship with such a customer.

4.10.5 Any match, or possible match to a PEP requires the MLRO’s approval and or further advice before allowing the customer to have an account with the Company. Should approval be granted for a PEP, enhanced due diligence may be required (such as additional documentation) but all PEPs will also be subject to ongoing monitoring of their account activity.

5. Risk-based approach methodology and control instruments

5.1 Company shall apply own instruments as union of tools within the FATFA recommendation, market peculiarities and technology risks in challenge and currently emerging within the Company market.

5.2. Company recognizes the risk of money laundering or terrorist financing is higher, and include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company’s business.

(b) Country or geographic risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.

- Anonymous transactions.
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties.

5.3. Company recognized lower risk given the good attitude and FATFA cooperating attitude within jurisdiction of the country or by the financial institution, simplified internet data register CDD measures, and shall be seen in the following:

(a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the
- Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

- When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, Company shall take into account risk variables relating to those risk categories:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions
-

- The regularity or duration of the business relationship.

5.5 Should the Clients' risk of the be considered low or should there be reasons to consider the risk of commercial relations low, a simplified control method of client identification may be used, by checking the data through the publically available databases that can be considered trustworthy. Aside from the low risk level that was given under the risk analysis following the provisions of part 5 of this Document, additional reasons to consider the transaction to be low risk are the following:

- the Client is a [company's country] public legal person;
- The Client is a state organization or another organization performing public functions that is acting in [company's country] or EU;
- the Client is an EU institution;
- the Client is a credit institution that is active in [company's country] and EU, where the provisions of directive 2015/849 are applicable.
- the Client is a physical person that is a resident of [company's country] or of country that has substantial anti-money laundering legislation following the Financial Action Task Force reports.
- the Client is appropriately defined physical person for limited services that Company provides and to certain types of customers, so as to increase access for financial inclusion purposes within an annual non-identified source personal transaction of less than USD/EUR 1,000 or a single payment less than USD/EUR 2,500.

Use of the simplified control method does not free the company from the obligation to make sure that the transaction is transparent.

5.6 The nature of the transaction must be evaluated to set the risk status.

5.6.1 The transaction may be awarded with a low, medium or high-risk status depending on the following factors:

5.6.2 Should the Client's risk be considered high or should there be reasons to consider the risk of commercial relations high, a higher-level control method of client identification should be used, by requesting the client to provide additional information and documents that can rule out the risk. Information is also to be provided to the financial inspection of Sent Lucia to get more instructions. Aside from the high-risk level that was given under the risk analysis following the provisions of part 5 of this Document, additional reasons to consider the transaction to be high risk are the following:

- unusual circumstances for the transactions;
- the client operates with high volumes of cash;
- a legal person client has hidden owners or recipient type shares;
- the structure of the legal person is too complex and confusing;
- new or unknown goods are the subject of the transaction and transaction specifics are unusual;
- the transaction is made for anonymity purposes;
- unknown third parties make payments following the transaction;
- Other circumstances mentioned in article 37 of the Money Laundering and Terrorist Financing Prevention Act.
- The transaction involves currency exchange or purchase of precious metals;
- The transaction involves a private bank;
- The transaction involves alternative payment methods;

- The transaction involves gambling;
- The transaction involves rarities or exclusive goods;
- The transaction involves innovations;
- The transaction involves commercials;
- The transaction involves company establishment or management.

5.7 Geographical circumstances are to be evaluated to determine a geographical risk of the transactions.

5.7.1 The transaction may be awarded with a low, medium or high-risk status depending on the following geographical actors:

- The transaction involves low tax jurisdictions. This entails a company registered at the low tax jurisdiction or services provided at the low tax jurisdiction;
- The transaction involves a state that does not cooperate in the field of money laundering prevention and finance of terrorism;
- The transaction involves a state with a high crime rate or trafficking of drugs;
- The transaction involves a state with a high level of corruption;
- The transaction involves a state that is subject to international sanctions;
- Other factors that may increase the geographical risk.

5.8 Along with the risks connected to the Client, risks regarding his partners or associated persons are also evaluated.

5.9 The risk evaluation is performed by giving each risk group a status on a three-point scale:

- Risk is considered low if no category has a risk factor and the transaction is clear;
- Risk is considered medium if there are risk factors, but the transaction itself is clear, though there are suspicions that all of the risk factors together may indicate money laundering or finance of terrorism;
- Risk is considered high if there are multiple risk factors and the transaction itself is not clear.

5.10 Overall result is achieved by adding the factor of each category, whereas risks regarding client and partner is multiplied by two and then the whole sum is divided by a factor of 4.

- If the sum is 2 or lower, the risk is low;
- If the sum is 2 to 2,75, the risk is medium;
- If the sum is higher than two are, 75, the risk is high.
- If the risk in any category is high, the overall risk is considered high no matter the overall sum.
- The MLRO and the Company Management team will carry out regular assessments of the risks posed by Company's Clients and the services provided by Company. The procedures set out in this Compliance Manual will be regularly assessed against the risks posed by Company's Clients.
- Company shall examine, as far as reasonably possible, the background and purpose of all high risk transaction (as but not limited: complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose where the risks of money laundering or terrorist financing are higher) and:

- Should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.
- Continuously asses similarity of such transactions with different groups of companies or related persons
- Amend own mythology to impede any illegal transaction being performed.

5.11 Company's applied controlling instruments for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

5.12.1 Company shall in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

(b) obtain senior management approval for establishing (or continuing, for existing ustomers) such business relationships;

(c) take reasonable measures to establish the source of wealth and source of funds; and

(d) conduct enhanced ongoing monitoring of the business relationship.

5.12.2 MLPO take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d). The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

6. Commercial relationship with the Client

6.1 Any commercial relationship with the Client is initiated only after the Client agreed to act in accordance with the present AML policy.

6.2 Before the start of commercial relationship the following must be set:

- Nature of the planned agreement;
- Terms of the planned agreement;
- Volume of the planned agreement.

6.3. Received information is kept in a written form.

6.4 Should there be a representative between a physical or legal person; the company is to ensure that there is actual contact between the client and the representative.

7. Actions in case of suspicions regarding money laundering and obligation to provide information

7.1 Should there be any suspicion before the initiation of commercial relationship or during the use of control methods, that the transactions may be connected to money laundering or finance of terrorism, further cooperation is impossible.

7.2 Any suspicions are registered and analyzed by the contact person. The Anti Money Laundering institution of Sent Lucia and the financial inspection of Sent Lucia must be notified immediately of the results of the analysis.

7.3 All information regarding any transactions that is 1000 EUR/USD or higher must be provided to the senior officers and financial institution managers.

7.4 Should the denial to perform the transaction result in damages to the Client or the arrest of a person suspected in money laundering or terrorism, the transaction may be delayed or performed on the condition that the Financial Inspection is informed immediately.

7.5 All the information provided to the Financial Inspection is kept in an archive in accordance with provision 13 of the present document, including the data analysis results.

7.6 Persons suspected of money laundering or the finance of terrorism should not be provided any information regarding the suspicions or notified of them by any other means.

8. Correspondence exchange

8.1 Should it be deemed by the management to be necessary to implement the control method, a correspondence exchange with third parties may be initiated, including banks and other financial institutions, should that allow to gather more accurate information.

8.2 The correspondence exchange must be drawn up in the form of a two-way agreement, including the control methods used.

8.3 There can be no correspondence exchange with shadow banks, unlicensed organizations or with organizations situated in jurisdictions whose legislation is not up to the international standards in the field of Anti money laundering legislation and prevention of the finance of terrorism.

8.4 Company with its financial counterparties shall take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

8.4.1 Company and financial counterparties should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

8.4.2 Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate.

8.4.3 Company and its financial counterparties shall take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmers and monitor them for compliance with these programmers.

9. Information recording program

9.1 Information recording program sets the obligation for the company employee who performed the transaction to draw up an internal document containing all the specifics of the transaction that must include:

9.1.1 The category of the transactions and the reasons why the transaction may be considered a high-risk transaction;

9.1.2 The details of the transactions, including the volume of the transaction and currency;

9.1.3 The details on the persons involved in the transactions;

9.1.4 The information on the Company employee involved and his signature;

9.1.5 The date of the act;

9.1.6 A written letter from the company management board member or from another authorized person regarding a transaction performed under this act.

9.1.7 Information regarding any additional methods of control used about the transactions;

9.1.8 There is no pre-arranged act form. Acts are made by hand by each employee and are presented to the member of the management board for review.

9.2 Company should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for prosecution of criminal activity.

9.2.1 Company shall be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

9.2.2 Company should be required by law to maintain records on transactions and information obtained through the CDD measures.

9.2.3 The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

10. Transaction denial program

10.1 If the Client, despite his obligation, did not present the required documentation in accordance with the control methods, the applicable legislation, and this policy, the Client will be denied in the performance of the transaction.

10.2 Should the Client fail to present information regarding the source of the funds upon the request, the transactions shall also be denied.

10.3 Information regarding the transaction denial must be kept in accordance with provision 13 of this policy, including:

- The information on the circumstances of the transaction denial and account blocking.
- The circumstances for the denial of the start of commercial cooperation;
- Any circumstances regarding the end of commercial cooperation in accordance with provisions 7.1 and 7.2 of the present policy.
- The data that provided the reason that the state authorities were notified in accordance with section 32 of the Money Laundering and Terrorist Financing Prevention Act.

10.4 The decision regarding the denial to perform the transaction may be reversed if the Client provides the required information and documents or if such shall be set by the decision of the following organs:

- A control organ of the [company's country];
- A competent Court [company's country].

11. Company employees training program

11.1 The program regarding the training of employees in the field of Anti Money Laundering Legislation and Prevention of the finance of terrorism is made in accordance to the applicable legislation and includes proper instructions for the employee regarding the control methods and information analysis. Any employee must be properly instructed by the authorised workers during the period of a month from the start of employment.

12. Internal control review program

12.1 The internal control review program ensures that the employees and members of the company abide by the provisions of the applicable legislation in the field of income legalization obtained by illegal means and the finance of terrorism. The program ensures that the employees abide by internal company rules and regulations in the field of internal control.

12.2 Internal controls set the following rules:

12.2.1 Regularly, at least once every six months, internal checks must be carried out regarding the proper implementation of internal regulations and applicable legislation.

12.2.2 Company member of the board must be provided with regular written reports regarding all the violations of internal regulations in the field of money laundering prevention and prevention of the finance of terrorism.

12.2.3 All violations revealed during checks must be properly handled by the means chosen by the management board member.

13. Document maintenance program

13.1 All documents connected to the client identification procedure as well as all the information regarding the start of commercial cooperation must be maintained in the company archive for no less than 5 years.

13.2 All documents that became the reason for notifying the state authorities must be maintained for no less than 5 years.

13.3 All information on the inquiries made in order to abide by the provisions of the applicable legislation must be kept for no less than 5 years from the start of commercial cooperation. If the identity was confirmed by the means of a digital document, then the picture of the person and their signature is kept for no less than 5 years from the date of the end of commercial cooperation.

13.4 The documents must be maintained in a form that allows their written reproduction, so that they would be readily available for financial control or for other state authorities in accordance with the applicable legislation, should they be required for use in civil, criminal, or arbitrary proceedings.

Internal control rules set the confidentiality standards for the information that was received during identification process and other means prescribed by the applicable legislation.