Attachment No 1 to of LUMA TRADING Ltd. Board of Directors Resolution

The Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT)

§1

Introduction

1. The Implementing Procedure is based on The Prevention of Money Laundering Act („**PMLA**") and the Prevention of Money Laundering and Funding of Terrorism Regulations which were issued by virtue of Legal Notice 372 of 2017 which came into force on 1 January 2018, („**PMLFTR**").
2. LUMA TRADING Ltd. with its registered office in St. Julians, Level 2, Luxe Pavilion, Portomaso Complex, (postal code: STJ 4010 St. Julians) Malta, incorporated under the Maltese law, registered by the Registrar of Companies under Registration Number: C72932, using the VAT no. MT23085034 (hereinafter referred to as: „**LUMA**" or „**the Company**") is the subject person.
3. LUMA shall be responsible for complying with the provisions of the PMLFTR, for performing and implementing the duties set out in the PMLFTR and for providing the information, notifications and reporting referred to herein.
4. The Procedure sets out the obligations and rules, that subject persons are required to fulfil and to implement, and without which an AML regime cannot be effective. It mainly consists of the following:
    a) procedures on internal control, risk assessment, risk management, compliance management and communications;
    b) customer due diligence;
    c) record keeping;
    d) reporting;
    e) training and awareness.
5. Every employee and associate of the Company shall be required to read the Procedure and to make an appropriate declaration, a draft of which is attached as an **Attachment No 1** to this Procedure.

§2

Risk assesment

1. A risk assesment is a process whereby the LUMA identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT risks.
2. The identification of the threats and vulnerabilities one is exposed to, requires a consideration of the risk areas and risk factors from a qualitative and a quantitative point of view. Thus, for the purposes of the Business Risk Assessments (hereinafter referred to as: „**BRA**"), LUMA shall consider how numerous these threats or vulnerabilities are.

3. There are some of the quantitative factors to be considered by LUMA for Business Risk Assessments:
   a) Customer Risk:
   i. the number of customers within each customer risk type;
   ii. the maturity of the client base, i.e., the duration of existing business relationships; and
   iii. the volume of business.
   b) Geographical Risk:
   i. the number of subsidiaries or branches within a given jurisdiction;
   ii. the number of customers and/or beneficial owners from a given jurisdiction;
   iii. the number of transactions to/from a given jurisdiction; and
   iv. the number of any other links that expose it to a given jurisdiction.
   c) Products, Services and Transaction Risk:
   i. the number of products, services (including correspondent and trade finance relationships) and transactions;
   ii. the number of customers per each product and service;
   iii. the volume per product and service.
   d) Delivery Channel:
   i. the number of relationships started on a non-face-to-face basis;
   ii. the number of distributors and agents; and
   iii. the number of customers introduced through introducers and intermediaries.
4. LUMA shall have to examine its current business structures, client base and portfolio of products and services, as well as any diversification or expansion plans may have.
5. Doing so LUMA will allow to identify the various risk factors that it is to take into consideration for its BRA. The combination and assessment of these risk factors will allow LUMA to identify the threats it is exposed to and the vulnerabilities that may be exploited for ML/FT purposes.
6. Having done so, LUMA will determine the likelihood of any one scenario materialising, and the possible impact thereof. Taken together, likelihood and impact will lead to one's inherent risk.
7. To assess the particular risk, LUMA implements Likelihood Scale according to §3, referring to the potential of an ML/FT risk occurring.

§3

Principles for identifying and assessing the risks of money laundering and terrorist financing relating to a given business relationship or occasional transaction.

1. For customers who have obtained a high risk classification, LUMA applies enhanced financial security measures as defined in the Procedure.
2. For customers who have achieved a low-risk qualification, LUMA may apply reduced financial security measures.
3. The Company updates the risk assessment in the event of:
   a) an update of the information held on a given customer;

b) whenever new threats and vulnerabilities are identified;
c) whenever there are changes to its business model/structures/activities;
d) whenever there is a change in the nature of relations between the Company and the customer, at least once every year.
e) whenever there are changes to the external environment within which the Company is operating.

4. The risk assessment is recorded on paper or electronically in accordance with the principles set out in the Procedure. The specimen form constitutes **Attachment No. 2** to the Procedure.

§4

1. Business or professional activities to be considered as presenting a high risk of ML/FT include cases when:

a) the activity pursued is cash (or cash equivalent) intensive;
b) the activity is commonly associated with a higher risk of corruption (e.g., the arms trade and defence industry, and the mining industry);
c) the activity is associated with a higher risk of ML/FT (e.g., virtual currencies and money remittance);
d) the activity is conducted through opaque and complex structures for which there does not seem to be a legitimate justification;
e) the customer is a personal asset-holding vehicle; or
f) the customer is a voluntary organisation that primarily engages in raising or disbursing funds for charitable, religious, cultural, educational or social purposes (especially when they remit funds to third countries), and hence its activities are particularly susceptible to be misused for the funding of terrorism;
g) commercial relations or occasional transaction is linked with:
   i. countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
   ii. countries identified by other credible sources as having serious deficiencies within their AML/CFT framework (e.g., FATF, FSRBs like MONEYVAL, IMF, etc.);
   iii. countries subject to sanctions, embargoes or similar measures issued by international organisations, such as the United Nations Security Council or the European Union. In addition, in some circumstances, countries subject to sanctions or measures that may not be universally recognised (e.g., OFAC sanctions) should be given credence by the subject person because of the standing of the issuer and the nature of the measures;
   iv. countries identified by credible sources as providing funding or support for terrorist activities or that have terrorist organisations operating within them;
   v. countries identified as having significant levels of corruption or other criminal activity through credible sources, like the Corruption Perception

Index compiled by Transparency International (The Corruption Perception Index is available through the website of Transparency International - https://www.transparency.org/);

vi. countries that have shown a lack of willingness to comply with international tax transparency and information sharing standards (e.g., failure to adhere to or apply the Common Reporting Standard); and

vii. countries that fail to implement effective beneficial ownership transparency and availability measures and hence allow the legal entities or arrangements set up in that jurisdiction to be used as s

2. ecretive vehicles and misused for ML/FT purposes.The high risk group includes also those LUMA customers with whom cooperation may imply an increased risk of money laundering and terrorist financing due to the risk factors analysed by LUMA concerning customers, countries or geographical areas, products, services, transactions or their delivery channels and other risk factors related to the business relationship or the occasional transaction, for example:
   1) the establishment of a business relationship in unusual circumstances;
   2) the circumstance that the customer of LUMA is:

a) legal person or an unincorporated organisational unit whose activities are used to hold personal assets,
b) a company in which bearer shares have been issued and whose be securities are not admitted to organised trading, or a company in which rights from shares are exercised by entities other than shareholders or shareholders,
c) a person holding a prominent political position, a person known to an associate of a person holding a prominent political position or a member of the family of a person holding a prominent political position;
d) the client's line of business involves carrying out a significant number or large amount of cash transactions;
e) unusual or excessively complex ownership structure of the client, taking into account the type and scope of his/her business activity;
f) the customer's use of services or products offered under private banking.

§5

The normal risk group includes those LUMA customers with whom cooperation can mean minimal or no risk of money laundering and terrorist financing.

§6

Business or professional activities to be considered as presenting a low risk of ML/FT include cases when:

a) entities are listed on a regulated market and are subject to enforceable disclosure requirements, which ensure adequate transparency of beneficial ownership;

b) entities carry out relevant financial business or equivalent activities subject to equivalent AML/CFT obligations as those applicable in Malta and which are subject to effective supervision; and
c) entities form part of the public administration or public enterprises.

§7

Customer due dilligence

1. Customer due dilligence (hereinafter referred to as: „**CDD**") measures ensures that LUMA have adequate mechanisms in place to:
a) determine who the customer and, where applicable, any beneficial owner are;
b) verify whether that person is the person he/she purports to be;
c) determine whether a person is acting on his/her own behalf or on behalf of another person (e.g., an agent, signatory, attorney, etc.);
d) establish the purpose and intended nature of the business relationship, and the customer's business and risk profile; and
e) in the case of a business relationship, monitor that relationship on an ongoing basis.
2. CDD measures shall apply to all customers when:
a) establishing a business relationship;
b) carrying out an occasional transaction;
c) the Company has knowledge or suspicion of proceeds of criminal activity, money laundering or the funding of terrorism, regardless of any derogation, exemption or threshold;
d) at appropriate times, to existing customers on arisk-sensitive basis and also whenever any of the following circumstances occur:
   i. when the Company becomes aware that the relevant circumstances surrounding a business relationship have changed;
   ii. when the Company has a legal duty to contact the customer for the purpose of reviewing and updating any information relating to the beneficial owners, including when the Company has such a duty in terms of the Cooperation With Other Jurisdiction On Tax Matters Regulations.
3. Customer due diligence measures shall be repeated whenever, in relation to a business relationship, doubts arise about the veracity or adequacy of the previously obtained customer identification information.
4. LUMA applies enhanced CDD in higher risk situations, such as:
a) when transacting with politically exposed persons;
b) in relation to activities or services that are determined by the Financial Intelligence Analysis Unit to represent a high risk of money laundering or funding of terrorism, having taken into consideration the findings of any national risk assessment and any other relevant factors as may be deemed appropriate;
c) in a cross-border correspondent banking relationship scenario, particularly when dealing with respondent institutions situated outside of the EU;

d) in the other cases referred to in sub-regulations (3) to (10) of point 11 of the Prevention of Money Laundering and Funding of Terrorism Regulations;
e) generally in any situation where there may be a grater risk of ML.

§8

Financial security measures

1. LUMA applies financial security measures to its customers to an extent and with an intensity that takes into account the identified risks of money laundering and terrorist financing associated with the business relationship or occasional transaction and its assessment.
2. LUMA documents the identified risk of money laundering and terrorist financing associated with the business relationship or occasional transaction and its assessment, taking into account the factors listed in § 2 point 3 of the Procedure.
3. Financial security measures include:

a) identification of the customer and verification of his identity;
b) identification of the beneficial owner and taking reasonable actions in order to:

i. verify of his identity,
ii. establish the structure of ownership and control - in the case of a customer who is a legal person, organisational unit without legal personality or a trust;
iii. assessment of the business relationship and, as appropriate, obtaining information on its purpose and intended nature;
iv. ongoing monitoring of the customer's business relationships, including:

a) analysing the transactions carried out in the business relationship to ensure that the transactions are consistent with the Company's knowledge of the customer, the nature and scope of the customer's business and consistent with the money laundering and terrorist financing risks associated with that customer,
b) investigating the source of wealth held by the customer, where justified by the circumstances,
c) ensuring that the documents, data or information held on the business relationship are kept up to date.

4. LUMA, in applying the financial security measures referred to in paragraph 3 points a) and b), identifies the person authorised to act on behalf of the client and verifies his/her identity and authorisation to act on behalf of the client.
5. LUMA documents the financial security measures applied and the results of the ongoing analysis of the transactions carried out to demonstrate that, given the level of identified risk of money laundering and terrorist financing associated with the business relationship or occasional transaction, LUMA has applied appropriate financial security measures. A model of the result of the current analysis of transactions constitutes **Attachment No. 3** to the Procedure.

§9

Identification of a LUMA customer

1. Identification of a LUMA customer consists in establishing, in the case of:

1) a natural person:

   a) name and surname;

   b) nationality;

   c) relevant number of the Public Electronic System of Population Records if applies or date of birth - if no Public Electronic System of Population Records number has been assigned, and country of birth;

   d) name and number of the document confirming identity of the person;

   e) address of residence - if this information is available;

   f) name (company), tax identification number and address of the main place of business activity - in case of a natural person conducting business activity;

2) legal person or organisational unit without legal personality, body corporate, a body of persons or any other form of legal entity:

   a) name (business name);

   b) organisational form;

   c) registered office address or business address;

   d) Tax Identification Number and if there is no such number - the country of registration, the name of the relevant register and the number and date of registration;

   e) identification data (name, surname, Public Electronic System of Population Records) of all directors and,where the legal person does not have directors, all such other persons vested with its administration and representation.

   2. The Company takes reasonable measures to verify the beneficial owners, including, in the case of a body corporate, foundations, trusts and similar legal arrangements, the taking of reasonable measures to understand the ownership and control structure of the customer.

   3. If the legal person or organisational unit without legal personality, body corporate, a body of persons or any other form of legal entity is subject to the registration of beneficial owner information, LUMA also obtains proof that such beneficial ownership information has been duly registered with a designated beneficial ownership register.

   4. Data verification is carried out on the basis of:

      1) the client's registration documents (obtained from relevant public official registers);

      2) public, official beneficial ownership register;

      3) data included in the identity card, in compliance with the rules resulting from the Personal Data policy binding in the Company;

4) concessions, licences, permits to conduct activities issued by competent authorities;

5) contracts, articles of association;

6) available internal databases.

§10

1. Identification of a person authorised to act on behalf of a client shall include: name, surname, nationality and Public Electronic System of Population Records number or date of birth where no Public Electronic System of Population Records number has been assigned and country of birth provided in a written form.
2. Identification of a person authorised to act on behalf of a client shall not release LUMA from a customer and beneficial owner identification.

§11

1. The verification of the identity of the customer, the person authorised to act on behalf of the customer and the beneficial owner shall consist in the confirmation of the identification data established on the basis of a document establishing the identity of the natural person, a document containing updated data from an extract from the competent register or other documents, data or information from a reliable and independent source, including, where available, from electronic identification means or from relevant trust services as defined in Regulation 910/214.
2. The Company shall verify the identity of the customer and, where applicable, the identity of the beneficial owner, before the establishment of a business relationship or the carrying out of an occasional transaction.
3. The verification of the identity of the customer and the beneficial owner may be completed at the start of the business relationship where this is necessary to ensure the continuity of the business and where there is a low risk of money laundering and terrorist financing. In such cases, verification shall be completed as soon as possible after the start of the business relationship.
4. Exceptionally the Company may complete the verification after the establishment of a business relationship where this is necessary so as not to interrupt the normal conduct of business provided that the risk of money laundering or the funding of terrorism is low and, provided further, that the verification procedures be completed as soon as is reasonably practicable after the establishment of the business relationship.

§12

1. In the event that LUMA cannot apply one of the financial security measures:

a) does not establish a business relationship;

b) does not carry out an occasional transaction;

c) does not carry out a transaction via a bank account;

d) dissolve the business relationship.

2. LUMA assesses whether the inapplicability of the financial security measures constitutes grounds for submitting to the Financial Intelligence Analysis Unit a report of circumstances that may indicate a suspicion of the commission of an offence of money laundering or terrorist financing or a notification of having a reasonable suspicion that a specific transaction or specific assets may be related to money laundering or terrorist financing.

§13

In the event of the disclosure of transactions that are unusual, unnaturally complex and involve large sums of money that do not appear to have any legal or economic justification, LUMA:

1) takes action to clarify the circumstances under which these transactions were carried out;

2) intensifies the application of the financial security measure with regard to the business relationships under which these transactions were carried out.

§14

Identification of politically exposed position (hereinafter referred to as: „PEP") and business relationship with such person

1. LUMA shall identify whether the client or the client's beneficial owner has PEP status.
2. Where the Company's client or beneficial owner is a person holding a politically exposed position, the Company shall implement procedures based on risk analysis, and shall accept a statement in written or documentary form (e-mail) that he is or is not a person holding such position, made under penalty of criminal liability for making a false statement. The person making the declaration is required to include the following clause: "I am aware of the criminal liability for making a false statement". This clause replaces the instruction on criminal liability for making a false declaration. Specimen declaration constitutes **Attachment No. 5** to this Procedure.
3. In the case of business relations with a person holding a politically exposed position, the Company applies financial security measures to such persons and takes the following actions:

a) the employee obtains the approval of the Management Board to establish or continue a business relationship with a person holding a politically exposed position;

b) establishes the sources of the client's property and the sources of the property values remaining at the client's disposal within the framework of the business relationship or transaction;
c) intensify the application of the financial security measure in the form of ongoing monitoring of the client's business relations.

4. In the period from the date on which a person ceases to occupy a politically exposed position until the date on which it is determined that no higher risk is associated with that person, but for no less than 12 months, the Company shall apply to such person measures taking into account that risk.
5. The above provisions shall apply mutatis mutandis to family members of the politically exposed person and persons known to be close associates of the politically exposed person.

§15

Rules for keeping records and information

1. The Company shall keep:

a) in relation to any business relationship that is formed or an occasional transaction that is carried out, the customer due diligence documentation, data and information obtained in fulfilment of the requirements under the Procedure;
b) supporting evidence and records necessary to reconstruct all transactions carried out by the Company in the course of a business relationship or any occasional transaction, which shall include original documents or other copies admissible in court proceedings;
c) a record of any disclosures made to the Financial Intelligence Analysis Unit in accordance with regulation 15 PMLFTR;
d) a record of any internal reports made in accordance with regulation 15(1)(a) PMLFTR;
e) a record of any written determinations made in accordance with regulation 15(1)(b) PMLFTR;
f) a record of any training provided in accordance with regulation 5(5)(e) PMLFTR; and
g) any other document, data or information which the Financial Intelligence Analysis Unit may require to be maintained in accordance with procedures and guidance issued in terms of regulation 17 PMLFTR

2. The Company shall keep documentation, data or information referred to in point (1) for a period of five years commencing on:
   a) in relation to the documentation, data or information described in paragraph (a) thereof, the date when the business relationship ends or when the occasional transaction is carried out, and where the formalities necessary to end a business relationship could not be observed, the date on which the last transaction in the course of that business relationship was carried out;
   b) in relation to the supporting evidence and records described in paragraph (b) thereof, the date when the business relationship ends or when the

occasional transaction is carried out, and where the formalities necessary to end a business relationship could not be observed, the date on which the last transaction in the course of that business relationship was carried out;

c) in relation to the records described in paragraphs (c) to (e), the later between the following:

i. the date when the business relationships ends or the occasional transaction is carried out; or

ii. the date when the report or determination is submitted or drawn up, as the case may be;

d) in relation to the records described in paragraph (f), the date when the event referred to therein took place.

§16

Principles for disseminating knowledge of anti-money laundering and counter-terrorist financing regulations to employees of the LUMA.

The Company ensures:

1) education persons performing duties related to the prevention of money laundering and financing of terrorism as regards the wording of The Prevention of Money Laundering Act (PMLA) and the Prevention of Money Laundering and Funding of Terrorism Regulations which were issued by virtue of Legal Notice 372 of 2017, linked regulations and any amendments thereof;
2) participation of persons, performing duties related to the prevention of money laundering and financing of terrorism, in training programs on the implementation of these duties, taking into account issues related to personal data protection;
3) legal consultations with the legal department on issues requiring clarification in the scope of the prevention of money laundering and financing of terrorism;

§17

Reporting procedures and obligations.

1. LUMA designates Krzysztof Matan as the reporting officer.
2. The reporting officer is a person to whom officers and employees of the Company are to report any information or other matter which may give rise to a knowledge or suspicion that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism.
3. Internal reports are to be submitted in writing to the reporting officer, together with all relevant information and documentation available to the employee. The report should

include details on the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

4. Every employee, who has any information referred to in point 2, shall report it the reporting officer, without delay.
5. The reporting officer shall have unrestricted access to any relevant information held by the Company.
6. The Company shall inform the Financial Intelligence Analysis Unit (hereinafter referred to as: „**FIAU**") about appointment of reporting officer, any amendments thereof.
7. The reporting officer submits a report to the FIAU whenever he determines that there is knowledge or suspicion that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism. Where, following the consideration, the reporting officer determines that no reporting to the FIAU is required in terms of this regulation, the reporting officer shall record the reasons for such determination in writing and, upon request, shall make it available to the FIAU or a supervisory authority acting on behalf of the FIAU in monitoring compliance with these regulations.
8. The report shall be given as soon as possible, but no later than 2 working days after the suspicion is confirmed.
9. The report shall include:
   1) the identification data of the Company's customer;
   2) possessed identification data of natural persons, legal persons and organisational units without legal personality, which are not clients of LUMA providing the report;
   3) type and size of property values and the place of their storage;
   4) the number of the account kept for the client of the Company providing the notification, marked with the IBAN identifier or identifier containing the country code and account number in the case of accounts not marked with IBAN;
   5) information in the possession of the Company with respect to the transaction or attempted transaction;
   6) the indication of the country of the European Economic Area, with which the transaction is connected, if the transaction was carried out within the framework of cross-border activity;
   7) information in the possession of the Company on the identified risk of money laundering or terrorist financing and the criminal act from which the assets may originate;
   8) a justification for the transmission of the report.
10. The reporting officer is also responsible for:
    a) responding promptly to any request for information made by the FIAU;
    b) ensuring continued compliance with the requirements of the PMLFTR, the FIAU's Implementing Procedures or other guidance issued by the FIAU;
    c) day-to-day oversight of the LUMA's AML/CFT measures, policies, controls and procedures;
    d) regular oversight reporting, including reporting of non-compliance, to senior management;
    e) addressing any FIAU feedback about the LUMA's risk management

f) performance or AML/CFT measures, policies, controls and procedures;
g) contributing to designing, implementing and maintaining internal AML/CFT compliance manuals, policies, procedures and systems;
h) conducting or seeing to periodic internal AML/CFT training for all relevant staff members and employees.

11. Where LUMA knows or suspects that a transaction is or may be related to proceeds of criminal activity or the funding of terrorism, the Company shall not carry out that transaction until it has informed the FIAU in accordance with this regulation and, upon informing the FIAU, it shall refrain from executing that transaction.
12. Where it is not possible for the Company to refrain from carrying out a transaction prior to informing the FIAU as provided for in point 8 or where refraining from carrying out any such transaction is likely to frustrate efforts of investigating or pursuing the beneficiaries of the suspected money laundering or funding of terrorism operations, the Company shall accordingly inform the FIAU immediately after the transaction is effected.
13. When the FIAU demands information from the Company, LUMA shall comply as soon as is reasonably practicable but not later than five working days from when the demand is first made. The FIAU may, where it deems so necessary, demand that the information be submitted within a shorter period of time.
14. If the reporting officer determines that no reporting to the FIAU is required aacording to PMLFTR, the reporting officer shall record the reasons for such determination in writing and, upon request, shall make it available to the FIAU or a supervisory authority acting on behalf of the FIAU in monitoring compliance with these regulations.

§18

Final provisions

1. This Procedure in its present wording shall enter into force as of the date of its introduction with effect from ....10 th December 2022
2. Any changes to this Procedure require a written form.

Attachment No 1 to the The Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT)

Declaration

I, the undersigned .... certify that:

1. I have familiarized myself with the Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT) which was implemented in LUMA TRADING Ltd.;
2. all doubts regarding the Procedure and its application have been explained to me;
3. I fully understand the provisions of the Procedure;
4. I undertake to comply with the Procedure;
5. I undertake to act in accordance with the Procedure in situations envisaged by the Procedure and by regulations on counteracting money laundering and terrorism financing;
6. I have been informed of the identity of the persons who have been designated to comply with the provisions of the Procedure;
7. I have been made aware by the Company of the anti-money laundering and counter-terrorist financing legislation;
8. I am aware of the details of the person to whom I may turn in the event of an obligation to report violations of anti-money laundering and terrorist financing legislation.

.....

(place, date)

.....

(signature of employee or associate)

Attachment No 2 to the The Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT)

CLIENT RISK FORM

The Client: .....

Risk assessment table, please circle the appropriate number of points in each category:

Type of client[1]	Geographical area	Type of product(s), service and method of distribution	Level of value of transactions carried out	Purpose, regularity or duration of the business relationship
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
----	10	----	---	---

Total points from the table:……

1) 5–7 points – risk reduced,
2) 8–13 points – normal risk,
3) 14 points and more – increased risk

CLIENT RISK ASSESSMENT:

REDUCED	NORMAL	INCREASED	NOT ACCEPTED[2]	PEP[3]

[1] Every risk factor shall include explanation for considering number of points

[2] Always mark the risk "not accepted" in cases referred to in the Procedure, in particular if the Client appears on sanctions lists.

[3] Board member approval required to enter into an agreement with the client. If the client has PEP status, the 'enhanced' rating should automatically be ticked.

Information sources used for Assesment:

.....

.....

date and signature of the employee carrying out the assessment

Attachment No 3 to the The Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT)

Draft of statement on the outcome of the ongoing review of transactions

..., day of ... year

I, the undersigned, ..., declare that in relation to ..... (designation of the Client), I have conducted a current analysis related to the business relationship or to the occasional transaction, taking into account factors regarding the type of Client, countries or geographical areas, purpose of the account, type of products, services, transactions or their delivery and distribution channels, level of assets deposited by the Client or value of transactions carried out, purpose, regularity or duration of the business relationship and other risk factors, related to the business relationship or to the occasional transaction, taking into account the previous knowledge of the Company about the Client and my professional and life experience.

In particular, the following activities were carried out by me

1) ongoing monitoring of the Client's business relations, including:

(a) analysing the transactions carried out in the business relationship to ensure that the transactions are consistent with the Company's knowledge of the Client, the nature and scope of the Client's business and consistent with the money laundering and terrorist financing risks associated with the Client,

b) to investigate the source of the assets at the disposal of the Client, where justified by the circumstances

c) ensuring that the documents, data or information held in respect of the business relationship are kept up to date.

After the current analysis, I have found / have not found (* tick as appropriate) ... suspicious transactions, which may be regarded as made for the purpose of money laundering and terrorist financing.

Risk classification of the Client (* tick as appropriate):

1) Low risk Client;

2) Client with higher risk level;

3) Client with normal risk level;

4) Client holding an exposed political position

On this basis I assess that the risk of money laundering and terrorist financing associated with the business relationship or occasional transactions with ... (Client designation) is as follows: normal risk/medium risk/high risk (* tick as appropriate).

.....

(date and signature)

Attachment No 4 to The Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT)

Draft of statement confirming the identification and verification of the Company's customer, the person authorised to act on its behalf and the beneficial owner.

I, the undersigned, confirm that I have performed the verification of:

1. The customer of the Company, with regard to the following data:

☐ Client - natural person:

(a) name and surname,

b) nationality,

c) number of the Universal Electronic System for Population Registration or date of birth - if no the Universal Electronic System for Population Registration number has been assigned,

(d) country of birth

e) series and number of the document confirming identity of the person,

f) address of residence - if the Company has this information,

☐ Client - natural person running business activity:

a) name (company),

b) tax identification number , and

c) address of the main place of business,

☐ Client - legal person or organisational unit without legal personality

(a) name (business name),

b) organisational form,

c) registered office or business address,

d) Tax Identification Number, and if there is no such number - the country of registration, the commercial register and the number and date of registration,

e) identification data (name, surname, the Universal Electronic System for Population Registration) of the person representing the legal person or organisational unit without legal personality.

☐ 2. the person authorised to act on behalf of the Company's customer, with regard to the following data:

(a) forename, surname,

b) nationality,

c) the Universal Electronic System for Population Registration number or date of birth

d) country of birth.

☐ 3. the beneficial owner, with regard to the following data:

(a) forename, surname,

(b) nationality

(c) the Universal Electronic System for Population Registration number or date of birth

d) country of birth,

(e) series and number of the identity document

f) address of residence.

The following discrepancies have been identified between the information collected in the Central Register of Actual Beneficiaries and the information on the client's actual beneficiaries established in connection with the application of the Act:

.....

Difficulties found in connection with the verification of the identity of the beneficial owner

.....

Actions taken in connection with the identification as a beneficial owner of an individual holding a senior management position:

.....

.....

(date and signature)

Attachment No 5 to The Prevention of Money Laundering (ML) and Funding of Terrorism Procedure (FT)

..., day of .....

Statement

I, the undersigned .....state that:

1) I am/am not * (delete as appropriate) a politically exposed person,

2) I am/am not * (delete as appropriate) a person known to be a close associate of a politically exposed person,

3) I am/am not * (delete as appropriate) a family member of a politically exposed person.

I am aware of the criminal responsibility for making a false statement.

.....

(date and signature of person making the statement)