



ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (“AML/CFT”) POLICY

VERSION 3 (ADOPTED 24 FEBRUARY 2022)

VERSION & REVIEW HISTORY

Version no.	Date:	Status:	Amendments made by:	Most important amendments:
1.1 for Contributors	14 Jul 2017	Adopted by BOD	N/A	N/A
1.2 for Borrowers	14 Jul 2017	Adopted by BOD	N/A	N/A
2.0	7 Dec 2020	Adopted by BOD	Intertrust,, Sail Ventures; approved by Simmons & Simmons	Combined AML Policies for Borrowers and Contributors into one policy.
3.0	24 Feb 2022	Adopted by BOD	Intertrust & Sail Ventures	<ul style="list-style-type: none">• Intertrust’s operational CDD tasks now relate to both Contributors and Borrowers;• More emphasis on <i>Wwft</i> & <i>Sanctiewet</i> framework
<i>Next review</i>	<i>February 2023</i>			

1. INTRODUCTION

This document shall set out the Fund’s policy with respect to the fight against money laundering and combating the financing of terrorism (“**AML/CFT**”) regarding the Customers of the Fund (the “**Policy**”). For the purposes of this Policy, Customer shall mean each of the contributors to the Fund (together the “**Contributors**” and each a “**Contributor**”) and each of the borrowers from the Fund (together the “**Borrowers**” and each a “**Borrower**”).

In addition to establishing the Fund’s risk framework for AML/CFT, the Policy will cover the following aspects:

- Governance of the Fund and description of the functions and responsibilities delegated by the Board of Directors (“**BOD**”) to the AML/CFT Compliance Officer (“**AMLCO**”).
- Description of the delegation by the AMLCO of the operational AML/CFT functions & duties with respect to the Customers delegated to INTERTRUST (NETHERLANDS) B.V. in its role as the Fund Administration service provider and Administrative Agent (“**AA**”) for the Fund, and the functions & duties to be undertaken by the AA in that regard.
- Description of the KYC and AML/CFT responsibilities of SAIL VENTURES B.V., in its role as the investment advisor of the Fund (“**IA**”) pursuant to the Investment Advisory Agreement as amended from time to time, signed between the Fund and the IA (“**IAA**”), to support the AA, and the functions & duties to be undertaken by the IA and AA in that regard.



1.1. Objective and implementation

The main objective of this Policy is to ensure that money laundering (“**ML**”) and terrorism financing (“**TF**”) risks in the process of fundraising for, and investments by, the Fund are properly identified, monitored, mitigated and reported in order to prevent the Fund and its Customers, governing bodies and service providers from being misused for ML/TF or any other financial misconduct or crime. Adherence to this AML/CFT Policy for Borrowers is also aimed at preventing the Fund from being exposed to reputational damage or financial loss for non-compliance with relevant regulatory standards.

The AA shall implement this Policy to ensure that the Fund complies and remains compliant with the relevant requirements of applicable Dutch AML/CFT laws and regulations.

Compliance with the Policy shall be subject to regular controls and verifications, at a frequency determined according to the ML/TF risks to which the Fund is exposed. The effectiveness of this Policy and procedure will be monitored and reviewed by the BOD periodically (as further described in **Clause 2**) and where necessary, taking into consideration its applicability and adequacy in the context of regulatory changes and operational capabilities and requirements of the Fund.

For the purpose of this Policy, certain terms or concepts related to AML/CFT that are not defined in the body of this Policy are explained in **Annex 7** (Definitions).

1.2. Legal framework

This Policy is based on the following legal framework (not exclusive and to the extent relevant):

- 1.2.1. The EU Fourth AML Directive 2015/849 and the revision thereto by Directive 2018/843;
- 1.2.2. The Dutch Money Laundering and Terrorist Financing (Prevention) Act (Wet ter voorkoming van witwassen en financieren van terrorisme) (“Wwft”);
- 1.2.3. The Implementing Decree Wwft 2018 (Uitvoeringsbesluit Wwft 2018);
- 1.2.4. The Implementing Regulations Wwft (Uitvoeringsregeling Wwft);
- 1.2.5. The Dutch Sanctions Act (Sanctiewet 1977) (“Sw”);
- 1.2.6. Guidance from European Supervisory Authorities, such as the Risk Factors Guidelines under articles 17 and 18(4) of EU Directive 2015/849;
- 1.2.7. Guidance from the Dutch Authority for Financial Markets (AFM Leidraad Wwft en Sanctiewet); and
- 1.2.8. The guidance from FATF Recommendations and subsequent guidance.



1.3. Deviation and waivers

It is possible to deviate from this Policy, in particular the acceptance procedure and requirements as set out in **Clause 5** and **Annex 1**, as far as allowed on the basis of the applicable laws and regulations. However, any material deviation or waiver requires a BOD decision based on advice from the AA and approval by the AMLCO. All material deviations and waivers are documented and stored in a retrievable manner.

2. GOVERNANCE OF THE FUND AND THE AML/CFT COMPLIANCE OFFICER (“AMLCO”)

2.1. Due to the relatively small size of the Fund (currently 4 non-executive board members, 5 non-executive advisory board (“**AB**”) members and no staff); the flat governance structure; the fact that the Fund is currently not regulated by any supervisory authority; and the fact that the Fund has outsourced part of its Customer due diligence (“**CDD**”) with respect to Customers to the AA and the IA (as set out below), the Fund currently does not have a dedicated compliance or internal audit function. However, as set out below, certain key persons have been charged with concrete responsibilities.

2.2. The BOD has the ultimate responsibility for all aspects of the administration and management of the business of the Fund. With respect to the AML/CFT framework, the BOD exercises its oversight in the following manner:

2.2.1. Approves and reviews this Policy if necessary and in any event annually.

2.2.2. Evaluates and (where applicable) updates the Business Risk Assessment (see **Clause 4**) if necessary and in any event annually.

2.2.3. Receives and discusses annual AML Reports and ad-hoc reports prepared by the AA on specific AML/CFT related measures.

2.2.4. If applicable, receives and reviews any auditor’s report on the appropriateness of the Fund’s AML/CFT framework and, where necessary, supervises the implementation of the audit findings and recommendations.

2.3. In order to facilitate the BOD monitoring of the Fund’s compliance with AML/CFT requirements under Dutch law, the BOD shall nominate and appoint at least one AMLCO from its members. The AMLCO, and ultimately the BOD, are responsible for AML/CFT matters.

2.3.1. Once appointed, the name of the AMLCO shall be communicated to the AB.

2.3.2. On 3 October 2017 the BOD resolved to appoint Mr. Nanno Kleiterp as the AMLCO of the Fund.

2.3.3. In the event that the AMLCO is not able to perform his/her function, any member of the BOD may act as the appointed alternate to, and temporarily replace, the AMLCO in his/her functions in order to ensure that the Fund complies with the AML/CFT legal and regulatory requirements.

2.4. AMLCO Requirements

2.4.1. The AMLCO shall have the professional experience and knowledge of the Dutch legal and regulatory framework relating to AML/CFT, the hierarchy and powers within the entity (including the power to access, on a timely basis, the identification



data of Customers and other information and documentation required by the due diligence measures).

2.4.2. The AMLCO needs to dedicate sufficient time to the effective and autonomous exercise of his/her functions.

2.4.3. The independence, objectivity and decision-making autonomy of the AMLCO shall not be impeded by their performance of any other function with respect to the Fund. His/her workload shall be adapted so that the efficiency of the AML/CFT framework is not compromised.

2.5. AMLCO Duties

2.5.1. The AMLCO has the power to suggest to the BOD, on his/her initiative, any necessary or useful measures, including the release of the required finances.

2.5.2. The AML/CFT policy shall be subject to initial validation and regular monitoring by the AMLCO in order to adapt it, where necessary, to the development of the activities, the Customers and the AML/CFT standards and measures.

2.5.3. The AMLCO monitors that the AA fulfills its obligations to the Fund regarding AML/CFT.

2.5.4. The AMLCO is in charge of monitoring the risks linked to AML/CFT based on the information provided by the AA in accordance with this Policy.

2.5.5. The AMLCO monitors that the AA has adequate AML personnel training programmes for the implementation of the AML/CFT framework.

2.5.6. The AMLCO is the main contact person for the competent authorities regarding AML/CFT compliance of the Fund (e.g. the competent supervisory authorities of the relevant Customers and the relevant Dutch authorities). He/she is also in charge of the reporting of any unusual transactions to these authorities and shall coordinate, to the extent applicable, with the Complaints Officer of the Fund.

2.5.7. The AMLCO has the right to start AML/CFT investigations on his or her own initiative, when deemed necessary.

2.5.8. The AMLCO shall be able to perform on-site visits, at reasonable times and upon reasonable notice, of any of the Fund's service providers (including the AA) and/or oversight reviews, if deemed necessary, in order to ensure the ongoing effective monitoring of the delegated AML/CFT functions.

2.5.9. The AMLCO shall provide a written report to the BOD on an annual basis and, if necessary, on an ad hoc basis.

2.5.10. The AMLCO shall remain abreast of relevant AML/CFT regulations and shall attend AML/CFT training, and procure that the members of all committees of the Fund attend AML/CFT training, on a regular basis, such that they are able to recognise unusual transactions and to perform adequate CDD (defined below). The AMLCO shall monitor the appropriateness of the training and awareness-raising programmes of the AA.



2.6. Reporting to the BOD

2.6.1. By 28 February of every year, and within ten business days of a written request from the AMLCO, the AA will each provide the AMLCO with a report containing the information required in order for the AMLCO to perform the above mentioned duties and to ensure that either there are no doubtful cases or that doubtful cases have been appropriately dealt with (each, an “**AML Report**”). A template of the AML Report is attached hereto as **Annex 2**.

2.6.2. Based on the AML Report, the AMLCO shall prepare, at least once a year, a summary report on his/her activities and his/her operation (the “**AMLCO Report**”). A template of the AMLCO Report is attached hereto as **Annex 3**.

2.6.3. The AMLCO Report shall include information provided by the AA and a confirmation from the AMLCO that he/she is comfortable with:

- the detail and implementation of the AML/CFT procedures applied by the AA;
- the level of professional knowledge and capacities of the AML/CFT team of the AA;
- the AML/CFT training program in place at the level of the AA.

2.6.4. The AMLCO Report shall include a confirmation from the AMLCO that:

- he/she is not aware of any unusual transactions with respect to AML/CFT matters;
- no communication has been made with any competent authorities with respect to AML/CFT aspects of the operations of the Fund;
- he/she has dedicated sufficient time during the past year to keeping him or herself up to date with the AML/CFT regulatory requirements.

2.6.5. The AMLCO Report shall include details of new and previously identified cases of AML/CFT problems, shortcomings and irregularities, their related risks and seriousness, the corrective actions proposed as well as a follow-up of recommendations made for previously identified issues. This includes a statement on the general positions of the persons concerned, an assessment of the scale of the ML/TF suspicions which may have been identified; and a judgment on the adequacy of this AML/CFT policy and of the collaboration between AMLCO, IA and the AA with regard to AML/CFT in each case.

2.6.6. If any of these items is absent, the report must describe the reasons for this absence and any remedial measures that may be deemed necessary in this respect.

2.6.7. The AMLCO Report shall be submitted to the BOD for approval during its first meeting each year.

2.7. Whistleblower policy

In terms of the Fund’s Code of Conduct (available on the [Fund’s website](#)), anyone working for or representing the Fund in any way, or any stakeholders (including Civil Society Organisations and representatives of affected communities) have the possibility to internally report violations of this Policy anonymously to the IA, or to the BOD or AB, as



may be appropriate. Further, the Complaints Management Policy (also available on the [Fund's website](#)) provides that complaints can be raised directly with the Complaints Officer.

3. DELEGATION OF AML/CFT FUNCTIONS & DUTIES TO THE AA AND THE IA

- 3.1. Pursuant to the Master Services Agreement, as amended from time to time, signed between the Fund and the AA, the Fund delegated certain operational AML/CFT duties/tasks to the AA. The AML/CFT functions provided by the AA are governed by the Master Services Agreement and this Policy, provided that the Fund remains responsible at all times for compliance with the applicable AML/CFT regulations. The AA undertakes the following operational AML/CFT duties/tasks:
 - 3.1.1. perform CDD and (as the case may be) periodic or event driven review (described below as Ongoing Due Diligence) on Customers, which includes an assessment of the risk of ML/TF associated with the Customers ;
 - 3.1.2. liaise with the IA on daily transaction of funds and monitoring anti-corruption, AML/CFT and good governance policies of the Fund; and
 - 3.1.3. keep up-to-date the necessary AML disclosures, filings and registrations required to be maintained on behalf of the Fund (including but not limited to the Registration of the Ultimate Beneficial Owners (“**UBO**”s), as outlined in **Annex 4**.
- 3.2. Without prejudice to his/her responsibility, the AMLCO may delegate the exercise of his/her functions to one or more departments/units/employees of the AA.
- 3.3. The AA and the IA shall cooperate with one another in good faith and each shall support the other in the implementation of its responsibilities in this Policy.

4. BUSINESS RISK ASSESSMENT

- 4.1. The Fund performs a regular business-wide risk assessment (the “**Business Risk Assessment**”). The Business Risk Assessment forms the basis for the Fund’s individual risk assessment and the subsequent policies to be implemented, in order to establish an appropriate level of CDD measures to be taken upon entering into individual business relationships with its Customers and ongoing monitoring.
- 4.2. For the purpose of this Policy, “**risk**” means the impact and likelihood of ML or TF taking place. For the Business Risk Assessment, the inherent risks are taken into account, which means the risk that exists before mitigation. Based on the identified inherent risks, the Fund has taken a number of general risk mitigating measures to address possible ML/TF risks. Any residual risks are addressed by conducting CDD with respect to individual Customers as set out in **Clause 5** and on an ongoing basis (Ongoing CDD, or ODD) by monitoring the relationship and the transactions in accordance with **Clause 7**.
- 4.3. The Business Risk Assessment takes into account risk factors relating to:
 - 4.3.1. risk of exposure to ML and/or TF,
 - 4.3.2. risk of exposure to bribery and or corruption,
 - 4.3.3. risk of exposure to Sanction law breaches,



4.3.4. the Fund's Customers,

- countries or geographic areas,
- products, services and transactions; and/or
- delivery channels.

4.4. Based on the Business Risk Assessment, the Fund applies a risk appetite framework to prepare Risk Appetite Statements for each Customer using the template attached hereto as **Annex 6**

5. CUSTOMER DUE DILIGENCE

5.1. Risk-based approach to CDD

5.1.1. Upon request from the IA or the AMLCO to conduct CDD on a (prospective) Customer, the first step is for the AA to assess the initial ML/TF risks associated with the Customer on the basis of the information available to the AA at that moment in time, using the Risk Based Approach set out in **Annex 1**. Following this assessment, each Customer will be allocated to one of the following categories:

- Customers to which low risk indicators apply, and to which no high risk indicators apply: the **Low Risk Category**;
- Customers to which one or more high risk indicators apply: the **High Risk Category**;
- in case neither low risk indicators nor high risk indicators apply: the **Normal Risk Category**.

5.1.2. The AA shall set the extent of the CDD measures according to the risk level assigned to each Customer in accordance with **Annex 1** and shall determine if Enhanced CDD (or EDD) measures are necessary.

5.1.3. The risk qualification shall take place during the identification period and shall continue afterwards in the framework of the ongoing monitoring. The risk category of a Customer may change as a consequence of performing the CDD with respect to that Customer: for instance if it appears to be difficult to obtain all relevant information from a Customer, or if it appears that the Customer, a representative or a UBO of the Customer, is a Politically Exposed Person ("**PEP**"). Each identified Red Flag, if assessed as material, will elevate the AML/CFT risk profile of a Customer with the corresponding consequence on the scope of CDD and monitoring.

5.2. Certain Customers may have ML/TF integrity risks associated with them that are unacceptable to the Fund. Without limitation, the Fund deems this to be the case if the CDD reveals that:

5.2.1. the identity of the Customer or its UBOs cannot be verified;

5.2.2. the Customer or its UBOs wish to stay anonymous, or provide fictitious identity information;

5.2.3. the Customer, an UBO or representative of the Customer appears on a Sanctions List;



- 5.2.4. the Customer does not provide, or provides insufficient, information regarding the nature and background of the Customer, and in particular the source of their wealth, if requested;
- 5.2.5. the organizational structure of the Customer appears, after research thereof, obscure, not transparent or unclear, and – taking into account the activities of the Customer – without clear underlying business rationale; or
- 5.2.6. where applicable, the Customer has not obtained the relevant licenses to conduct its business.

5.3. Acceptance of a new Customer

- 5.3.1. The AA shall report the results of the CDD to the AMCLO, who shall present the results of the CDD to the BOD.
- 5.3.2. The BOD shall decide whether or not to conduct business with a prospective Customer. It shall thereby observe the results of the CDD performed. The BOD shall not accept a Customer where:
 - the CDD has not been completed;
 - the ML/TF integrity risks in connection with the Customer are considered unacceptable by the BOD, in consultation with the AMLCO.

5.4. CDD process

- 5.4.1. For the purposes of the identification of Customers, and in relation to the appropriate level of CDD determined by the risk assessment, the AA shall gather and register at least the information set out in **Annex 5**.
- 5.4.2. The CDD process should enable the AA to:
 - identify the Customer and verify the identity of the Customer;
 - identify the UBO(s) (as defined in Annex 6) and take reasonable measures to verify the identity of the UBO;
 - if the Customer is a legal entity, take reasonable measures to understand the ownership and control structure of the Customer, including identifying any shareholders holding more than 25% of common equity and, if a shareholder holds more than 25% of the common equity, to continue to identify upstream shareholder(s) owning more than 25% of the common equity until, if applicable, the level of the UBO (such shareholders, UBO('s) and the authorized representatives of a Customer collectively referred to as the **“Connected Parties”**);
 - establish the goal and intended nature of the business relationship;
 - verify that any person purporting to act on behalf of the Customer is so authorised and identify and verify the identity of that person;
 - take reasonable measures to verify that the Customer acts for itself or for the benefit of a third party. In that regard, the Customers shall sign an explicit declaration and shall undertake to immediately communicate any subsequent changes to the Fund; and



- in the event of Normal or High Risk, gather and register, at the time of the Customer identification, information about the origin of the Customer's funds.

5.4.3. Once the Customer has been accepted, the CDD should enable the Fund to have a continuous control on the business relationship and the transactions conducted during the business relationship in order to ensure that these transactions correspond with the knowledge the entity has of the client and its risk profile.

5.5. Sanctions Checks

The AA will check to ensure that no new Customer nor any Connected Parties appear on any sanction list, including but not limited to the following (each a "**Sanction List**"):

5.5.1. **United Nations:** The lists of sanctioned persons promulgated by the United Nations Security Council, or its committees, pursuant to resolutions issued under Chapter VII of the United Nations Charter as well as in connection with ML or anti-terrorism matters, including:

"The List established and maintained by the Committee pursuant to resolutions 1267 (1999) and 1989 (2011) with respect to individuals, groups, undertakings and other entities associated with Al-Qaida"

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

"United Nations Security Council resolution issued under Chapter VII of the UN Charter or on the World Bank Listing of Ineligible Persons"

<https://www.un.org/securitycouncil/sanctions/2374/materials>

5.5.2. **European Union:** The lists of sanctioned persons issued by the European Union pursuant to Article 215 of the Treaty on functioning of the European Union, as available on the official EU websites:

"Consolidated list of persons, groups and entities"

http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm

5.5.3. **Netherlands:** Dutch national terrorism list

<https://www.rijksoverheid.nl/documenten/rapporten/2015/08/27/nationale-terrorisraelijst>

5.6. Integrity Check

5.6.1. In addition to Sanctions List checks, the AA will screen its the Customer and its Connected Parties on three (3) other aspects:

- Political exposure (i.e. identify PEP's)
- Negative media; and
- country risk

5.6.2. The AA uses an application that is integrated with the well-known global screening database World Check, which provides the input to screen on the above aspects



5.7. Keyword searches

5.7.1. The AA will also perform a Google keyword search of the potential Customers, UBO's and Connected Parties via the relevant public search engines and conduct a headline scan of the top 5 search results ("**Headline Scan**"). The top 5 screen results of the Headline Scan shall be maintained as part of the Customer's CDD file.

5.7.2. In addition, should any notable directly related article(s) appear from the Headline Scan), the AA shall review and save the text of such direct article coverage as part of the CDD file ("**Media Search**").

5.8. Timing of identification and verification

5.8.1. The AA cannot open a capital account designated for a prospective Customer's contribution before the Customer has been accepted by the BOD as a Customer.

5.8.2. However, for Customers for whom there is clear evidence of a reduced risk of ML/TF, an account can be opened before acceptance by the Fund provided that:

- sufficient comfort has been obtained on the identity of the Customer;
- at least the simple copies of the KYC documents of the Customer and, if applicable, the UBO have been received together with a structure chart disclosing the structure up to the top-entity or UBO; and
- no realization and transfer of funds from the account can be carried out before having completed the CDD procedure.

5.8.3. The verification of the identity is carried out at the earliest opportunity after the first contact with the Customer and sufficient measures shall be put in place so that no realisation and transfer of funds from the account can be carried out before completing this verification.

5.9. Customer in the process of incorporation

5.9.1. The AA shall identify and verify the identity of the Customer's founders and shall require a written and signed declaration from the founders stating that they act, either in their own name or on behalf of underlying Customers which they name, and where appropriate, the AA shall take measures to identify and verify the identity of the underlying Customers.

5.9.2. At the earliest opportunity after the incorporation of the Customer, the AA shall complete the measures for the identification and verification of the Customer's identity through information and documents of the UBO. The impossibility to verify the identity of the persons concerned within the timeframe set by the internal rules shall be subject to an internal report which will be transmitted to the AMLCO for the required purposes.

5.9.3. Sufficient measures shall be put in place so that no realization and transfer of funds from the account can be carried out before completing this verification.

5.10. Record-keeping

5.10.1. The record-keeping obligation covers all documents and information obtained under the CDD measures including:



- the results of any performed analysis;
- the written reports transmitted to the AMLCO;
- documents and information relating to transactions;
- the analysis of the transactions and facts included in the reports;
- the decisions taken accordingly; and
- the results of any other performed analysis.

5.10.2. The record-keeping of the documents may be carried out on any archiving medium, provided that the documents meet the conditions to be used as evidence in a judicial procedure or investigation; or any analysis of ML/TF by the competent authorities as regards AML/CFT issues.

5.10.3. The Fund retains all of the information that is gathered in the framework of CDD and ODD for a period of five (5) years from the end of the business relationship with the relevant Customer. The Fund has outsourced the recording and filing of this information to the AA and (where applicable) the IA.

5.11. Adequate Internal Management

5.11.1. The AA shall have procedures and implement control mechanisms that allow them, when conducting the risk assessment and monitoring the transaction, to identify the Customers and cash flows.

5.11.2. The AA shall ensure that each staff member fulfils the criteria of adequate AA standing and experience according to the risk of ML/TF related to the duties and functions to be carried out.

5.11.3. The AA shall ensure that its staff is regularly trained, following an appropriate AML/CFT training and awareness-raising measures.

5.11.4. The AA procedures shall include the conditions, deadlines and steps for the Customer relationship manager to communicate reports to the AMLCO.

5.11.5. The AA shall conduct annual checks and confirm that their relevant operations' comply with the applicable provisions as regards the prevention of ML/TF.

6. SPECIFIC AML/CFT RESPONSIBILITIES WITH RESPECT TO BORROWERS

In addition to the provisions of **Clause 5**, the following provisions shall apply to Borrowers:

- 6.1. In accordance with the IAA and part D.f.iii of Fund's Operations Memorandum, approved and amended by the BOD from time to time, the AA shall always be supported by the IA in conducting a CDD on any new Borrower with respect to whom the IA submits a credit application to the Fund Credit Committee, and the IA shall include a summary report on the CDD in the credit application.
- 6.2. In addition to the assessment of Borrowers existing AML/CFT/risk management practices the IA also takes due steps, with the support of the AA, to assure ongoing compliance with Fund's AML/CFT standards.



- 6.3. The IA ensures that the respective financing documents shall include adequate provisions to ensure Borrower's compliance or commitment to comply in all respects with all local standards and regulations, the FATF standards and recommendations as well as with internal procedures and controls, for the purpose of preventing the Borrower or the Fund from becoming an instrument for ML/TF, fraud or other corrupt or illegal purposes or practices. Such provisions typically include:
 - 6.3.1. Representation on compliance with laws;
 - 6.3.2. Representation on acting in its own name and for its own account;
 - 6.3.3. Information undertaking on KYC, AML and similar procedures;
 - 6.3.4. Undertaking to comply with local and, where relevant, EU laws, regulations and standards regarding anti-money laundering, combating the financing of terrorism and prevention of prohibited conduct standards and regulations and the FATF standards and recommendations;
 - 6.3.5. Undertaking not to engage in prohibited conduct (including money laundering and terrorism financing);
 - 6.3.6. Undertaking to implement, maintain and comply with (i) internal procedures and controls satisfactory to the Lender for the purpose of preventing becoming an instrument for any prohibited conduct and (ii) a corresponding effective compliance system, and
 - 6.3.7. Corresponding information and access rights.
- 6.4. The IA will also obtain confirmation regarding the valid execution of the relevant lending documentation by the Borrowers and relevant contractual parties, satisfaction of conditions precedents and any other documents required by the relevant lending documentation.
- 6.5. For each new Borrower, the IA shall include, in the credit proposals presented to the Credit Committee, the following:
 - 6.5.1. a section describing the AML/CFT or applicable risk management checks and due diligence performed by the AA on the Borrower;
 - 6.5.2. the main findings with respect to the Borrower's AML/CFT policy or other applicable risk management procedures and processes.
- 6.6. At reasonable intervals, and where required by the AA, the IA confirms the existence, and - if applicable - valid execution, of the relevant investment documentation by the Borrower. The content of such confirmation depends on factors such as the type of transaction, the instrument in which the Fund invests, the country of origin and the nature of the Borrower. Therefore, the confirmation includes the review of the relevant corporate documents of the Borrower, comprising of the articles of association (or similar documents), register extracts and other relevant local law documents.

7. MONITORING AND ONGOING DUE DILIGENCE

- 7.1. The Fund continuously monitors the business relationship with a Customer and the transactions performed by or on behalf of a Customer, to ensure that they are in line



with the Fund’s knowledge of the Customer, including its financial situation and its risk profile. The monitoring shall include the detection of any implausible origin of funds by comparing the declarations made by the Customer during the acceptance procedure with the actual origin of their funds.

7.2. Periodic and event-driven reviews of CDD

7.2.1. The ongoing due diligence on the Customers (“**ODD**”) includes the obligation to verify and, where appropriate, to update, periodically in accordance with the risk categorisation, the documents, data or information gathered on the Customer and its UBOs while fulfilling the CDD obligations, and the documents, data and information shall be verified and updated immediately when a suspicion arises.

7.2.2. The AA will conduct Ad-hoc/Event-driven reviews of the Customer’s ML/TF risk profile triggered by shareholder/UBO changes, media alerts, negative events, imposition of sanctions etc., which can also result in re-assessment of the Customer’s risk profile.

7.3. Termination of business relationship

The relationship with an existing Customer for whom the risk classification has been adjusted to ‘Unacceptable’ (e.g. due to changes in such Customer’s situation), must be terminated as soon as possible. The BOD, with assistance from the AA and the IA, will determine how the Fund can carefully phase out the relationship with the Customer within a reasonable period of time. In the interim, adequate mitigating actions need to be taken, such as blocking further disbursements to such Customer.

7.4. Review calendar

The frequency of the periodic ODD review depends on the risk category of the relevant Customer:

Risk category	Low Risk	Medium Risk	High Risk
CDD Scope	Simplified	Standard	Enhanced
Monitoring frequency	Once every three (3) years	Once every two (2) years	Annually

8. SUSPICION OF ML/TF ACTIVITIES

8.1. In the process of applying this Policy and only to the extent permitted by law, employees and/or contractual third party service providers of the AA must immediately notify the AMLCO of any activity that has been identified by them as unusual in the context of AML/CFT, detailing the reason for suspicion and providing any and all relevant information. In the event that the unusual activity relates to the AMLCO, then the employee and/or contractual third party service providers shall notify another member of the BOD.

8.2. The AMLCO shall, without delay, determine whether an investigation is required by the Fund, with the purpose and goal of the investigation being to identify and understand the background to unusual activities and ascertain whether the origin of funds and identity



of the Customer, any underlying contributor, UBO or transferee, is plausible. The investigation may include, but is not limited to, a review of all records from the initial CDD review, historical transactions, discussions with legal counsel and other managers involved in the transaction, though not with employees of the Customer.

- 8.3. If, after such investigation and consultation with the AMLCO, the origin of funds or identity of the Customer, any underlying contributor, UBO or transferee, appears to be still implausible or suggests criminal behaviour, the AMLCO will be notified and must determine whether or not an external report to competent authorities is required based on all available information.
- 8.4. The AMLCO is also required to investigate unusual activities of which he/she becomes directly aware and to decide, on the basis of all available information and additional investigations, whether or not the transaction/instruction remains suspicious or whether there is some additional information that removes the suspicion.
- 8.5. All reported suspicions, regardless of the ultimate action taken by the AMLCO, must be submitted to the BOD and the report along with any other relevant documentation, especially the document explaining the reasoning behind the decision taken, must be retained by the AMLCO.
- 8.6. The AMLCO shall be able to answer quickly and comprehensively all information requests from the competent authorities with regards to AML/CFT matters.



LIST OF ANNEXES

- ANNEX 1: RISK BASED APPROACH TO AML/CFT
- ANNEX 2: AML REPORT TEMPLATE (*PROVIDED BY THE AA*)
- ANNEX 3: ANNUAL REPORT PROVIDED BY THE AMLCO TEMPLATE
- ANNEX 4: REGISTRATION OF BENEFICIAL OWNERS
- ANNEX 5: KYC FOR CUSTOMERS
- ANNEX 6: RISK APPETITE STATEMENT
- ANNEX 7: DEFINITIONS



ANNEX 1: RISK-BASED APPROACH TO AML/CFT

The Fund uses a Risk-based assessment approach in the process of assessing the initial eligibility of potential Customers, from the AML/CFT risk perspective, as well as performing an ongoing monitoring of the risk status of all existing Customers. The Risk-based assessment approach ensures a more appropriate allocation of resources and yields a better result by channeling more attention to High Risk Customers and determining the level of CDD that is required.

For each potential Customer the AA shall perform a risk assessment and attribute a corresponding risk level (**Low, Medium, High** or **Unacceptable**) based on a range of risk factors.

The factors described below are not exhaustive and the AA may also categorize a Customer as High risk even if none of the listed High risk factors apply. To the extent permitted by law, the AA may categorize a Customer as Medium or Low risk Customer if one or more High risk factors applies, for instance if there are other factors in relation to the Customer that lead to lower ML/TF risks.

The risk classification of a Customer will determine the level of the CDD that is applied (**Simplified, Normal** or **Enhanced**), and the respective monitoring frequency as set out in **Clause 7**.

1. Risk Factors

1.1. Transaction Risk

- 1.1.1. The Fund is not offering any products or services nor engages in transactions which inherently pose direct ML/TF risks (i.e. cash-intensive products such as payment services or current accounts).
- 1.1.2. Furthermore, the Fund predominantly engages in financing of companies directly or indirectly involved in agricultural commodity production, either by providing direct financing or via financial intermediaries.
- 1.1.3. The Fund does not engage in financing structures which are unnecessarily more complex than what is required to achieve the objective of the transaction.
- 1.1.4. Nevertheless, when considering investments, the Fund takes reasonable measures to duly assess the purpose, intended nature, economic rationale and overall AML/CFT aspects of the business relationship in order to avoid being involved in business relationships structured for the purposes of criminal activities or co-financed through funds of possibly illicit origin.

1.2. Geographic (jurisdiction/country) risk factors

- 1.2.1. With respect to the geographic (jurisdiction/country) risk of the potential Customer, the AA shall consider the risk with reference to the country in which the Customer is incorporated or has its main place of business.
- 1.2.2. The factors considered in determining a High level of ML/TF related country risk, may include:
 - Countries of higher risk, as mentioned in the country list issued by the European Commission as countries which have strategic deficiencies in their AML/CFT regimes;



- Countries of higher risk, as mentioned by the FATF as 'Jurisdictions under Increased Monitoring';
- Countries on the EU and/or Dutch list of non-cooperative tax jurisdictions.
- Countries identified as providing funding or support for terrorists, or their activities;
- Countries identified as having significant levels of criminal activity, including corruption and drug trafficking;
- Countries facing a protracted period of political instability;
- Countries not being cooperative in terms of tax transparency;
- Countries subject to sanctions, embargo or similar measures imposed by the UN, EU or US (OFAC);
- **High** AML index, high corruption and crime rates (as established by the Basel Institute of Governance or Transparency International).

1.2.3. The AA will regularly consult a range of relevant sources to access the risk level of each country of operation, which may include:

- mutual evaluation reports by the FATF or FATF-style Regional Bodies (FSRBs),
- the FATF's list of high-risk and non-cooperative jurisdictions,
- European Commission lists of high-risk third countries having strategic deficiencies in their regime on AML/CFT;
- Transparency International (Corruption Perceptions Index);
- Basel AML Index annual reports.

1.3. Customer-specific risk factors

1.3.1. **High** Risk Category

The factors that may determine a **High** level of ML/TF related client risk may include:

- Ownership, structure and corporate governance of the Customer: unnecessarily complex/non-transparent organizational structure; corporate governance practices raising doubt, negative track record/integrity of stakeholders;
- Identification and reputation of UBOs and other key stakeholders: difficulties in identification of UBOs, (if applicable) unclear source of wealth of UBOs, negative legal record and/or severe public allegations against beneficiaries and management, etc.;
- Other integrity risk concerns related to Customer: Nominee shareholders or bearer shares in shareholder or governance structure of the Customer, confirmed negative legal track record/severe public allegations, misconduct/direct and indirect unethical practices, evident links to organized crime, etc.;
- The UBO or legal representative of a Customer is considered to be a PEP;



- Customer -specific business model and related exposure to ML/TF risk: significant exposure to high ML risk sectors (such as project finance), clearing operations, operations with high-value items and value redistribution, complicated high- net worth transaction and private wealth management etc.;
- Customers with identified weaknesses in the adequacy and effectiveness of their own AML/CFT Framework or risk management framework.

1.3.2. **Low** Risk Category

A Customer is considered to be a Low risk only after a case-by-case evaluation. The following factors are generally considered indications of a Low risk, unless the CDD results in an assessment to the contrary:

- Regulated credit and financial institutions, including pension funds, subject to adequate AML/CTF regulations;
- Listed company on a recognized stock exchange (EU, UK, US, New Zealand, Australia, Japan, Singapore, South Korea, South Africa, Switzerland, Israel);
- Non-listed entities that are a 100% subsidiary of a listed company on a recognized stock exchange;
- Government institutions or majority-owned stated-owned enterprises from the EU, EEA or equivalent low risk jurisdictions (UK, US, New Zealand, Australia, Japan, Singapore, South Korea, South Africa, Switzerland, Israel); and

(The Contributors in the Fund are typically considered to have a Low risk, as they are regulated entities, government institutions and/or listed companies based in the EU or an equivalent Low risk Jurisdiction.)

1.3.3. **Normal** Risk

Customers that are not classified as Low or High risk are classified as Normal risk.

2. Risk Categories

- 2.1. Each of the above risk factors and sub-factors shall be assigned a score and weighting which reflects the level of risk associated with that risk factor and the prevalence of that risk compared to other risk factors.
- 2.2. Each Customer will be assigned a corresponding ML/TF risk category: **Low, Medium, High** or **Unacceptable**. The level of CDD applied is captured in the below table and is based on the Risk classification of the Customer:
 - 2.2.1. **Low** Risk: this triggers Simplified Due Diligence (“**SDD**”)
 - 2.2.2. **Normal** Risk: this triggers Normal Due Diligence (“**NDD**”)
 - 2.2.3. **High** Risk: this triggers Enhanced Due Diligence (“**EDD**”)
 - 2.2.4. **Unacceptable**: this triggers a decision not to start or to terminate the business relationship with the Customer.



3. Client Due Diligence

CDD Requirements	SDD	NDD	EDD
Integrity check and risk assessment:			
Customer identification	✓	✓	✓
Database screening	✓	✓	✓
Extended research of other publicly available sources		✓	✓
Commissioning external background study ¹			✓
Assessment of the adequacy of the local regulatory framework	✓	✓	✓
Assessment of Borrower ML/TF policies and procedures:			
Standardized AML Questionnaire prepared by the IA	✓	✓	✓
Additional detailed /targeted questionnaires on Customer's AML/CFT/risk management framework, organization, structure and capacities prepared by the IA		✓	✓
Additional off-site review of Customer's relevant AML/CFT/risk management policies and procedures, compliance & internal audit reports			✓
Additional on-site interviews with key credit, compliance and internal audit personnel of Customers performed by the IA			✓
Documentary due diligence			
Collection and verification of relevant corporate constitutional documents, licenses and approvals as well as various identification documents and signing authorities	✓	✓	✓

3.1. SDD

During an SDD the AA will apply the same level of due diligence as NDD, with the exception of information on the source of funds of the Customer and the performance of Google keyword searches.

3.2. EDD

3.2.1. Customers that are in scope for High risk indicators as described in **Clause 1** above shall be subject to the EDD procedure and corresponding mitigating measures, including increased monitoring frequency.

3.2.2. The AA applies the following enhanced CDD procedure:

- together with the IA request the Customer to provide additional information on the intended nature of the transactions that are carried out during the business relationship; and
- where the UBO or representative of a Customer is a PEP or where the Customer is established in a higher risk jurisdiction as listed by the European Commission, together with the IA obtain additional information to establish the source of wealth of the Customer and source of funds of the transaction(s) with the Customer or (as the case may be) PEP.

¹ Commissioned only in specific cases, typically where specific ML/TF Red-flags point to a Higher risk profile



3.2.3. In the event that a business relationship with a (prospective) Customer involves:

- a PEP at the level of the Customer, UBO or its authorized representative; or
- a country with a deficient AML/CFT framework (High Risk jurisdiction),

then the AA shall inform the AMLCO and request explicit approval of the acceptance of such PEP or (as the case may be) High Risk jurisdiction. Such AMLCO approval is a separate and mandatory step before proceeding with acceptance of the Customer.

3.2.4. The following additional measures may also be applied by the AA:

- together with the IA, request the Customer to provide copies of CDD documents that are used to verify the identity of the Customer, its UBO or representative(s) that are certified as a true copy by a registered notary, lawyer or accountant; and
- if deemed necessary, request the AMLCO to commission an external background study including:
 - additional information on the Customer (ownership, key shareholders)
 - origins or sources of the Customer's wealth and sources of funds linked to the relevant transaction(s) with the Customer;
 - local and international reputation of the Customer;
 - ongoing or concluded litigation and/or confirmation of allegations of criminal offenses or involvement in ML/TF practices;
 - questionable business practices in other ventures;

4. PEP Assessment

- 4.1. The definition of a PEP is set out in Annex 7.
- 4.2. The procedures to determine whether a Customer, its authorized representative or UBO is a PEP may include, among others, seeking relevant information from the Customer, referring to publicly available information or having access to electronic databases of PEPs.
- 4.3. PEP Assessment of Contributors
- 4.3.1. The Fund acknowledges and understands that PEP's require EDD as they are deemed to pose higher risks in relation to possible corruption due to their prominent and influential functions.
- 4.3.2. The Fund may enter into business relationships and receive funding from Contributors that are government institutions or majority-owned stated-owned enterprises ("SOE's") from EU, or equivalent low risk jurisdictions. These are indicators of Low risk. However, at the level of the pseudo UBO(s) or authorized representative(s) of such Contributor persons are likely to qualify as PEP, which triggers EDD.
- 4.3.3. If the sole reason for the PEP status is the identification of a person as pseudo UBO or authorized representative of a government or SOE from a Low risk jurisdiction then:



- after applying EDD (including BOD approval); and
- if no other High risk factors apply,

the Customer is scored as Low Risk, as the Fund deems that ML/TF risks associated with these PEP's will be Low as well.



ANNEX 2: AML REPORT TEMPLATE (provided by the AA)

STICHTING ANDGREEN.FUND (the "Fund")

REPORT TO THE AML/CFT COMPLIANCE OFFICER ON AML/CFT MATTERS

To : AML Compliance Officer (the "**AMLCO**")
From : Intertrust (Netherlands) B.V. ("**AA**")
Date : [DATE], presented by the AMLCO at the Board meeting held on [DATE]

The AML/CFT confirmation provided by the **AA** for the period [PERIOD] ("Period"), attached hereto as Annex 1, confirms that:

- the AA has been delegated the CDD procedure for Customers
- the Customers of the Fund have been identified in accordance with the Fund's policy;
- the number of Enhanced Due Diligence Customers in the Period was: [number]
- the number of unusual transactions/activities by Customers that were noticed by the AA in the Period was: [number]
- to the extent permitted by law, the Fund will be notified on any unusual transactions/activities in relation to Customers that are noticed by the AA in performing the delegated services under the Fund's policy.

Customer	Customer Type	Risk profile	Review frequency	Last review	Next review

[DATE]

Signature



ANNEX 3: ANNUAL REPORT PROVIDED BY THE AMLCO TEMPLATE

STICHTING ANDGREEN.FUND (the "Fund")

REPORT ON AML/CFT MATTERS PREPARED BY THE AML/CFT COMPLIANCE OFFICER

To : Members of the Board of Directors of the Fund (the "Board")
From : [NAME], AML/CFT Compliance Officer ("AMLCO")
Date : [DATE], presented at the Board meeting held on [DATE]

Items related to AML/CFT matters to be brought to the attention of the Board: [N/A]
No such instances have been brought to the attention of the AMLCO.

The AML/CFT confirmation provided by the AA for the period [PERIOD] ("Period"), attached hereto as Annex 1, confirms that:

- the contributors in the Fund ("Contributors") have been identified in accordance with the Fund's policy;
- the borrowers from the Fund ("Borrowers") have been identified in accordance with the Fund's policy;
- the number of Enhanced Due Diligence Contributors in the Period was: [number]
- the number of Enhanced Due Diligence Borrowers in the Period was: [number]
- the number of unusual transactions/activities by Contributors and/or Borrowers that were noticed in the Period was: [number]
- the Fund will be notified on any unusual transactions/activities by Contributors and/or Borrowers that are noticed by the AA in performing the delegated services under the Fund's policy..

In addition, the AMLCO hereby confirms that he/she is comfortable with:

- the detail and implementation of the AML/CFT procedures of the AA;
- the level of professional knowledge and capacities of the AML/CFT team of the AA; and
- the AML/CFT training program in place at the AA.

Furthermore, the AMLCO confirms that:

- he/she is not aware of any unusual transactions with respect to AML/CFT matters;
- he/she has not been in contact with any competent authorities with respect to AML/CFT aspects of the Fund's operations;
- he/she has dedicated sufficient time during the past year to keeping him or herself up-to-date with the AML/CFT regulatory requirements.

[DATE]

Signature



ANNEX 4: REGISTRATION OF BENEFICIAL OWNERS

Under Dutch law, with effect from 27 September 2020 the Fund is required to register its Ultimate Beneficial Owner (“**UBO**”) in the dedicated register (“**UBO register**”) maintained by the Dutch Chamber of Commerce (the “**KvK**”) and to update or amend such registration when necessary.

The Fund has delegated the UBO registration process to Intertrust as the AA and it has been agreed between Intertrust and the Fund that any registration of a new UBO, or any change in UBO data, will be managed as follows:

- In connection with the first registration of an UBO, or of any change in a UBO’s data, the Fund, through its Investment Advisor (“IA”) or Fund Management Advisor (“FMA”) will inform the AA by means of a form containing at least the following mandatory information with respect to each UBO:
 - a) the name;
 - b) the surname(s);
 - c) the nationality(ies);
 - d) the day, month, year and place of birth;
 - e) the country of residence;
 - f) the exact private address or professional address;
 - g) the identification number assigned to individuals’ resident in the Netherlands and registered with the Netherlands register of natural persons (“*Basisregistratie personen*”, “**BRP**”);
 - h) the national identification number as provided on the relevant individuals’ identification document and/or passport in the event the UBO is not residing in the Netherlands and consequently not registered with the BRP; and
 - i) the type and extent of beneficial interests held;
- AA will check the UBO register to determine if the new UBO or new UBO data has been registered by another party (such as the notary) and, if so, that the correct data has been registered.
- In the case that an UBO, or new UBO data, has not been registered, the AA will file the above-mentioned information with the required supporting documents (i.e. ID documents), within the relevant timeframe from the time when the Fund became aware or should have known of the event triggering the necessity of registration or modification of any UBO information.
- AA will report back to the Fund by sending a copy of the proof of registration by e-mail to the IA and FMA.
- The Fund, AA and the IA undertake to inform each other of any change in the structure or organisation that could potentially lead to a change in UBO or in the data with respect to an existing UBO.



National authorities as defined in the relevant Dutch Law relating to UBO, including but not limited to the tax, customs, registration, title and VAT authorities shall have unlimited access to all the information present in the UBO register, in the performance of their duties.

The Fund shall obtain, and keep at its registered office, current, accurate and constantly updated information on its UBO. The information must be provided to national authorities, within three business days of a simple request, and to professionals subject to KYC obligations in the context of AML/CFT (banks, asset managers, among others) upon a reasonable request.

The Fund shall designate the place where the information and the supporting documents will be kept for a period of five years from the date on which the registered entity has been removed from the KvK, in case of a dissolution. The designation of the place of storage shall be published in the KvK.



ANNEX 5: KYC FOR CUSTOMERS

Type	CDD	Verification
Natural	<ul style="list-style-type: none"> • surname and first name, • place and date of birth, • nationality, • address and country of residence, • official national identification number / passport (where available); 	<ul style="list-style-type: none"> • Address verification • Passport, ID or residence permit (<i>one valid official identification document issued by a public authority and which bears the Contributor's signature and picture</i>)
Legal	<ul style="list-style-type: none"> • Full name and trading name • legal form, • jurisdiction of incorporation • address of the registered office • principal place of business, if different from registered address • official national identification number (where available) • constitutional documents (certificates of incorporation, memorandum and articles of association (as well as any amendments), • annual report and/or last audited accounts [<i>if applicable</i>] • register of commerce or any document issued by a local authority [<i>if applicable</i>] • Operating license [<i>if applicable</i>] • List of authorized signatories • Statement confirming signatory authorization • Confirmation of good tax standing (FATCA/CRS self-certification [<i>if applicable</i>]) • Register of shareholders and directors • Structure chart including detail of the shareholder structure (showing at least all shareholders holding more than 10% of common equity), • Copy of passports and evidence of registered address of directors and UBOs of the legal entity. • Determine if acting on behalf of others 	<ul style="list-style-type: none"> • Address verification • Current articles of incorporation • Confirmation of good tax standing • Current extract from the company's shareholder/owner register or structure chart
Trust	<ul style="list-style-type: none"> • Requirements for Legal PLUS • Settlers Information (Natural / Legal), • Trustees Information (Natural / Legal) • Beneficiaries Information (Natural / Legal) • Protector Information (Natural / Legal) (if applicable) 	<ul style="list-style-type: none"> • Requirements for Legal
Fund	<ul style="list-style-type: none"> • Requirements for Legal PLUS • Investors' Information (Natural / Legal), • Fund Manager's Information (Natural / Legal), 	<ul style="list-style-type: none"> • Requirements for Legal



ANNEX 6: RISK APPETITE STATEMENT

Risk Appetite Topic	Risk Appetite Statement
AML	
CFF	
Anti-Bribery and Corruption (" ABC ")	
Tax (evasion)	
Sanction Laws	
Country risk	
Business sector risk	
Corporate Social Responsibility	

[Table included as a reference, Risk Appetite Statements to be updated once the Business Risk Assessment has been finalized.]



ANNEX 7: DEFINITIONS

Financial Action Task Force on Money Laundering (FATF) is an inter-Governmental body whose purpose is the development and promotion of policies to combat ML. Its membership includes the major financial center countries of Europe, North and South America and Asia.

FATF List of high-risk and other monitored jurisdictions: on the basis of the results of the review by the International Co-operation Review Group (ICRG), the FATF identifies jurisdictions with strategic AML/CFT deficiencies in the following public documents that are issued three times a year: FATF Public Statement (call for action) and Improving Global AML/CFT Compliance: Ongoing Process (other monitored jurisdictions).

Financing of Terrorism (FT) means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 3 to 10 of Directive (EU) 2017/541 of 15 March 2017 on combating terrorism. Where the Financing of Terrorism concerns any of the offences laid down in articles 3, 4 and 9 of Directive (EU) 2017/541, it shall not be necessary that the funds be in fact used, in full or in part, to commit, or to contribute to the commission of, any of those offences, nor shall it be required that the offender knows for which specific offence or offences the funds are to be used.

Money Laundering (ML) denotes the following conduct, when committed intentionally:

- the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Politically Exposed Person (PEP) means a natural person who is, or who, in the previous twelve months, has been entrusted with, prominent public functions and includes the following:

- 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 other high-level judicial bodies, 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, chargés 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 organization.



PEP status also extends to family relationships and persons known as close associates of a PEP. Family relationships of a PEP are:

- The spouse of a PEP or a person acting as an equivalent to the spouse of a PEP;
- A child of a PEP, the spouse of that child or a person who is considered equivalent to the spouse of that child;
- The parent of a PEP;

Persons known as close associates of a PEP are:

- A natural person who is known to be the joint UBO of a legal entity or a legal structure with a PEP, or who has other close business relationships with a PEP;
- A natural person who is the UBO of a legal entity or legal arrangement known to be established for the actual benefit of a PEP;

No public function referred to in this list shall be understood as covering middle-ranking or more junior officials.

Any PEP that retires from their prominent public function shall be assessed by the AA as to whether they are still a PEP and a proposal in that regard made to the AMLCO for a decision.

Red Flags mean additional ML/TF and Integrity risk factors including:

- Conviction of a serious crime, ongoing criminal investigation, or credible evidence of existing links to organized crime and criminal activities of the Customer's UBO or of any member of the management or board of directors.
- Investigations or sanctions/fines by regulatory bodies, such as financial oversight authorities, are Red Flags which need to be carefully evaluated before proceeding. Disclosure of actions by regulatory bodies, such as regulatory fines or sanctions against existing clients, upon becoming aware thereof, must be brought to the attention of the Fund's relevant decision-making body.
- Business relationships with PEPs or with other high-risk clients may expose the Fund to higher reputational risks. These persons may either be in a position to exert undue influence on decisions regarding the conduct of business by private sector parties or have access to state accounts and funds. In addition, PEPs and high-risk clients may be vulnerable in case of regime change.
- In addition to the principles described above, the Fund avoids entering an investment where there is evidence of involvement in poor, questionable or dubious business practices. Examples of such practices might include, but are not limited to, significant failure to comply with material local legal and regulatory requirements, allegations of involvement in fraud, tax evasion, bribery or corruption practices, etc.

Risk-Based Assessment of the Customer's own AML/CFT Framework takes into account whether the Customer's jurisdiction is a High Risk Jurisdiction, whether any PEPs are in the Customer's ownership or governance structure, the presence of any Red Flags, the adequacy of the local regulatory framework, particularly the application of the recommendations made by the Financial Action Task Force (FATF) and the level of compliance of the Customer's policies and controls with local and international standards. In the absence of a proper local regulatory framework, attention is paid during the due diligence process to the Customer's own policies and procedures addressing these areas



Ultimate Beneficial Owner (UBO) means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and,

in the case of corporate entities, includes:

- the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity. A shareholding of 25% plus one share or an ownership interest of more than 25% in the Customer held by a natural person shall be an indication of direct ownership. A shareholding of 25% plus one share or an ownership interest of more than 25 % in the Customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership.
- if, no natural person can be identified as a Beneficial Owner in accordance with the above criteria, or if there is a doubt as to whether the identified persons are the UBOs, the natural person acting as the senior managing official(s) shall be identified.

in the case of a partnership, a shipping company, a European economic interest grouping or any other entity comparable to a partnership, includes:

- natural persons who ultimately own or control the entity, through:
 - a) direct or indirect ownership of more than 25% of the ownership interest in the entity;
 - b) the ability to exercise directly or indirectly more than 25% of the voting rights in the decision-making to amend the agreement that the entity is based on, or in the case of the performance of that agreement other than through acts of management, to the extent that that agreement provides for a majority voting requirement for resolutions to be passed; or
 - c) the ability to exercise effective control over the entity; or
- if, after having exhausted all possible means, none of the persons referred to in subsection (i) is identified, the natural person(s) who are the partners (vennoten) of the partnership, excluding limited partners (stille vennoten);

in the case of a trust or other legal arrangement similar to a trust:

- the settlor(s);
- the trustee(s) or person(s) acting on behalf of the entity;
- the protector(s), if any;
- the beneficiaries, or where the individuals benefiting from the trust or the entity cannot be determined, the class of persons in whose main interest the trust or the entity is set up or operates; and
- any other natural person exercising ultimate control over the trust or the entity by means of direct or indirect ownership or by other means;