+31 (0)70 744 8884
info@andgreen.fund
www.andgreen.fund

Basisweg 10, 1043AP
Amsterdam, The Netherlands

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

VERSION 5 (ADOPTED ON 19 MAY 2026)

VERSION & REVIEW HISTORY

Version no.:	Date:	Status:	Amendments made by:	Most important amendments:
1.1 for Contributors	14 July 2017	Adopted by BOD	N/A	N/A
1.1 for Borrowers	14 July 2017	Adopted by BOD	N/A	N/A
2.0	7 December 2020	Adopted by BOD	CSC and SAIL (reviewed by Simmons & Simmons)	Combined the AML/CFT policies for Borrowers and Contributors into one policy.
3.0	24 February 2022	Adopted by BOD	CSC and SAIL	• CSC's operational CDD tasks now relate to both Contributors and Borrowers; • More emphasis on the *Wwft* & *Sanctiewet* framework.
4.0	9 December 2025	Adopted by BOD	CSC and SAIL	• Conversion of the AML/CFT policy into an &Green framework policy; • Legal, regulatory and operational updates.
5.0	19 May 2026	Adopted by BOD	CSC and SAIL	• Changes to the frequency of the ongoing customer due diligence (ODD) on low-risk and medium-risk Customers for alignment with CSC's new operating manual and KYC tool (iKYC).
Next review: Q1 2027				

KEY DEFINITIONS

Defined Term	Definition
AMLCO	AML/CFT Compliance Officer
BOD	the board of directors of the Stichting
Borrower	a borrower of the Stichting, BV1 or BV2 (as the case may be)
BV1	&Green Fund B.V.
BV2	&Green Fund Vehicle B.V.
BVs	collectively, BV1 and BV2
Contributor	a contributor of funds (whether by way of a grant, a loan or otherwise) to the Stichting
Customer	a Contributor, Noteholder, Borrower or Guarantor
Fund	collectively, the Stichting and the BVs

Guarantor	a guarantor in a financing transaction entered into by the Stichting, BV1 or BV2 with a Borrower
Management Body	the board of directors of each of the Stichting, BV1 and BV2 and, if the context requires, such boards of directors collectively
Noteholder	an investor in notes issued by BV2
Stichting	Stichting andgreen.fund

1. INTRODUCTION

This document sets 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**").

In addition to establishing the Fund's risk framework for AML/CFT, the Policy covers the following aspects of the Fund's AML/CFT framework:

- Governance of the Fund and description of the functions and responsibilities delegated by the Management Body to the AMLCO;
- Description of: (a) the delegation by the AMLCO of the operational AML/CFT functions and duties with respect to the Customers to Intertrust (Netherlands) B.V. in its role as the fund administration service provider and administrative agent ("**AA**") of the Fund; and (b) the functions and duties to be undertaken by the AA in that regard; and
- Description of: (a) the AML/CFT responsibilities of Sail Investments B.V. ("**SAIL**"), being the investment advisor or investment manager (as the case may be) of the entities forming the Fund, in each case pursuant to the relevant investment advisory or investment management agreement (as amended from time to time); and (b) the functions and duties to be undertaken by SAIL in that regard with a view to supporting the AA in the performance of its AML/CFT functions and duties with respect to the Fund.

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, Management 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 and Guarantors is also aimed at preventing the Fund from being exposed to reputational damage or financial loss for non-compliance with the 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 and European Union ("**EU**") 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 the procedures described herein will be monitored and reviewed by the Management Body periodically (as further described in **Clause 2**), taking into account (as necessary and appropriate): (a) the legal and regulatory requirements applicable to the Fund; (b) the operational capabilities of the Fund; and (c) the adequacy

of this Policy and the procedures described herein in the context of legal and regulatory changes in the area of AML/CFT.

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 6** (*Definitions*).

1.2. Legal and regulatory framework

This Policy is based (without limitation) on the following legal and regulatory framework (in each case, to the extent applicable to the Fund):

1.2.1. Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and the revisions thereto by (*inter alia*) Directive (EU) 2018/843 (until repealed);

1.2.2. Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (as from 10 July 2027);

1.2.3. the Dutch Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*) ("**Wwft**"), which, *inter alia*, transposed Directive (EU) 2015/849 into Dutch domestic law (as amended or replaced from time to time);

1.2.4. the Implementing Decree Wwft 2018 (*Uitvoeringsbesluit Wwft 2018*);

1.2.5. the Implementing Regulations Wwft (*Uitvoeringsregeling Wwft*);

1.2.6. the Dutch Sanctions Act (*Sanctiewet 1977*);

1.2.7. the guidance from the European Supervisory Authorities, such as the Risk Factors Guidelines under articles 17 and 18(4) of Directive (EU) 2015/849;

1.2.8. the Dutch Central Bank (*De Nederlandsche Bank*) *Wwft* Q&As and Good Practices; and

1.2.9. the guidance from the Financial Action Task Force ("**FATF**") Recommendations and subsequent FATF or similar guidance.

1.3. Deviation and waivers

It is possible to deviate from this Policy, in particular the Customer 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 Management Body decision based on advice from the AA and the prior approval of the AMLCO. All material deviations and waivers are documented and stored in a retrievable manner.

2. AML/CFT GOVERNANCE OF THE FUND

2.1. Due to (a) the relatively small size of the Fund in terms of assets under management, (b) the absence of staff employed by the Fund, (c) the non-executive nature of the majority of the members of the Management Bodies and the Fund's advisory board ("**AB**"), (d) the fact that the Fund is not currently regulated by any supervisory authority and (e) the fact that the AMLCO has outsourced the operational AML/CFT functions and duties with respect to the Customers to the AA (with support from SAIL, where applicable), the Fund currently does not have a dedicated compliance and/or internal audit function. However,

as set out below, certain key persons have been charged with concrete relevant responsibilities.

2.2. The Management Body 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 Management Body 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. reviews and signs off on the CDD performed on a Customer further to escalation by the AMLCO in accordance with **Clause 5.3.2**;

2.2.4. receives and discusses the annual AML/CFT reports and any *ad hoc* reports submitted to the Management Body by the AMLCO;

2.2.5. receives and discusses the annual AML/CFT reports and any *ad hoc* reports prepared by the AA on specific AML/CFT-related measures; and

2.2.6. if applicable, receives and reviews any auditor's report on the adequacy of the Fund's AML/CFT framework and, where necessary, supervises the implementation of the audit findings and recommendations.

2.3. In order to optimise the monitoring of the Fund's compliance with the applicable AML/CFT requirements under Dutch and EU law, the Management Bodies shall collectively nominate and appoint an AMLCO from the members of the BOD, such that a single AMLCO is appointed for the Fund. The AMLCO, and ultimately the Management Bodies, shall be responsible for AML/CFT matters relating to the Fund.

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

2.3.2. In the event that the AMLCO is not able to perform his/her functions, any other 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 applicable AML/CFT legal and regulatory requirements.

2.4. <u>AMLCO Requirements</u>

2.4.1. The AMLCO shall have the requisite professional experience and knowledge of the Dutch and EU legal and regulatory framework relating to AML/CFT, as well as the necessary powers within the Fund (including the power to access, on a timely basis, the identification data of Customers and other information and documentation required by the applicable Customer due diligence measures) in order to perform his/her AML/CFT functions.

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 his/her performance of any other function with respect to the Fund or otherwise. His/her workload shall be adapted so that the effective

performance of his/her duties under the Fund's AML/CFT framework is not compromised.

2.5. AMLCO Duties

2.5.1. The AMLCO has the power to suggest to the Management Body, on his/her initiative, any necessary or useful AML/CFT 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 of the Fund, the Customers and the applicable AML/CFT standards and measures from time to time.

2.5.3. The AMLCO monitors that the AA fulfils 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/CFT personnel training programmes for the implementation of the AML/CFT framework of the Fund.

2.5.6. To the extent required by applicable AML/CFT laws and regulations, the AMLCO is the main contact person for the competent authorities regarding the 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 the Financial Intelligence Unit – the Netherlands ("**FIU-Nederland**").

2.5.7. The AMLCO has the power 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 one single written report to the Management Bodies on an annual basis and, if necessary, also on an *ad hoc* basis.

2.5.10. The AMLCO shall remain abreast of relevant AML/CFT laws and regulations and shall attend regular (at least annual) AML/CFT training and procure that all delegates of the Fund performing AML/CFT functions attend regular (at least annual) AML/CFT training, such that they are able to identify unusual transactions and properly perform their respective AML/CFT duties. The AMLCO shall monitor the appropriateness of the training and awareness-raising programmes of the AA.

2.6. Reporting to the Management Body

2.6.1. By 28 February of every calendar year, and within ten business days of a written request from the AMLCO, the AA will 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 have been no unusual cases or that unusual 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 framework applied by the AA;
- the level of professional knowledge and capacity of the AML/CFT team at the AA; and
- the AML/CFT training programme in place at the AA.

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

- he/she is not aware of any unusual transactions with respect to AML/CFT matters and/or any identified unusual transactions have been appropriately dealt with in accordance with applicable AML/CFT laws and regulations;
- no report has been made to any competent authorities with respect to the AML/CFT aspects of the operations of the Fund or, if applicable, any such required report has been made in accordance with applicable AML/CFT laws and regulations; and
- he/she has dedicated sufficient time during the past year to keeping himself or herself up-to-date with the AML/CFT legal and regulatory requirements applicable to the Fund.

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 and/or taken 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 the AMLCO and the AA with regard to AML/CFT matters 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 Management Body for approval at its first meeting in each calendar year.

2.7. Whistleblower policy

Pursuant to 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 right to report

violations of this Policy anonymously to the Management Body, SAIL or the AB, as may be appropriate. Furthermore, the Complaints Management Policy (also available on the Fund's website) provides that complaints can be raised directly with the Fund's complaints officer.

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

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 performed 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 laws and regulations. The AA undertakes the following operational AML/CFT duties/tasks:

3.1.1. perform customer due diligence ("**CDD**") and (as the case may be) periodic or event-driven review (described below as "ongoing customer due diligence (ODD)") on Customers, which includes an assessment of the risk of ML/TF associated with the Customers;

3.1.2. liaise with SAIL on daily transactions of funds and monitor the implementation of the anti-corruption, AML/CFT and good governance policies of the Fund; and

3.1.3. keep up-to-date the necessary AML/CFT 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) of the Fund, as outlined in **Annex 4**.

3.2. Without prejudice to his/her responsibility, the AMLCO may delegate the exercise of any of his/her operational functions (other than his/her supervisory functions hereunder) to one or more departments/units/employees of the AA.

3.3. The AA and SAIL shall cooperate with one another in good faith and each shall support the other in the implementation of 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 for the purposes of the ongoing monitoring thereof.

4.2. For the purposes 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 risks that exist 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; and

4.3.4. the Customers'

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

5. CUSTOMER DUE DILIGENCE

5.1. Risk-based approach to CDD

5.1.1. Upon request from SAIL 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 point 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 to be applied 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, or a representative or UBO of the Customer, is a Politically Exposed Person ("**PEP**"). Each identified Red Flag (as defined in **Annex 6**), if assessed as material, will elevate the AML/CFT risk profile of a Customer with the corresponding consequences on the scope of the applicable CDD and the ongoing AML/CFT monitoring of such Customer.

5.2. Certain Customers may have ML/TF integrity risks associated with them that are 'Unacceptable' to the Fund. Without limitation, the Fund shall deem 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, or a UBO or representative of the Customer, appears on a Sanctions List (as defined below);

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 organisational structure of the Customer appears, after research thereof, obscure, not transparent or unclear, and – taking into account the activities of the Customer – without a clear underlying business rationale; and/or

5.2.6. where applicable, the Customer has not obtained the requisite licences to conduct its business.

5.3. Acceptance of a new Customer

5.3.1. The AA shall report the results of each CDD to the AMCLO. The AMLCO shall then review such results and revert to the AA with comments or sign off on such CDD. By signing off on the results of the CDD performed by the AA on a Customer, the AMLCO shall be deemed to have accepted such Customer from an AML/CFT perspective.

5.3.2. If the AMLCO deems it necessary or advisable, he/she shall escalate to the Management Body any AML/CFT concerns arising from the CDD performed on a Customer. In this case, the Management Body shall be responsible to sign off on the CDD performed on such Customer and accept such Customer from an AML/CFT perspective.

5.3.3. Notwithstanding the above, the AMLCO or the Management Body (as applicable) shall not accept a Customer where:

- the CDD in respect of such Customer has not been completed; and/or
- the ML/TF integrity risks in connection with such Customer are considered 'Unacceptable' by the AMLCO or the Management Body (as applicable).

5.4. CDD process

5.4.1. For the purposes of the identification of Customers, and in relation to the appropriate level of CDD as 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) of the Customer 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 authorised representatives of a Customer being collectively referred to as the "**Connected Parties**");

- establish the goal and intended nature of the business relationship with the Fund;
- 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 of 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 Customer 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 sanctions list, including but not limited to the following (each a "**Sanctions List**"):

5.5.1. **United Nations**: The lists of sanctioned persons promulgated by the United Nations Security Council, or its sanctions committees, pursuant to resolutions issued under Chapter VII of the United Nations Charter as well as in connection with ML or TF matters, including (without limitation) the United Nations Security Council Consolidated List:

https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list

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

EU Sanctions Map

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

https://www.rijksoverheid.nl/documenten/rapporten/2015/08/27/nationale-terrorismelijst

5.6. Integrity Checks

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

- political exposure (*i.e.*, identify PEPs);
- 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 Customers and their Connected Parties on the above aspects.

5.7. Keyword searches

5.7.1. The AA will also perform a Google keyword search of the potential Customers, UBOs, authorised representatives 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 in 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 AMLCO or the Management Body (as applicable) 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 on behalf of the Fund provided that:

- sufficient comfort has been obtained on the identity of the Customer;
- at least simple copies of the "know your customer" ("**KYC"**) documents of the Customer and, if applicable, its UBO(s) have been received together with a structure chart disclosing the structure up to the top-entity or UBO(s); and
- no realisation and transfer of funds from the account can be carried out before the CDD procedure is complete.

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 this verification is complete.

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 by obtaining information and documents on the Customer's UBO(s). The impossibility (if any) to verify the identity of the persons concerned within the timeframe set by the AA 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 this verification is complete.

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 collected under the Fund's AML/CFT framework 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 investigation by the competent authorities as regards AML/CFT issues.

5.10.3. The Fund retains all of the information that is gathered within 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 record-keeping of this information to the AA and (where applicable) SAIL.

5.11. Adequate Internal Management

5.11.1. The AA shall have procedures and implement control mechanisms that allow it, when conducting the AML/CFT risk assessment and monitoring the relevant transaction(s) or business relationship(s), to identify the Customers and the relevant cash flows.

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

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 to the AMLCO that its relevant operations comply with the applicable legal and regulatory 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. The AA shall always be supported by SAIL in conducting a CDD on any new Borrower with respect to whom SAIL submits a final proposal to the investment committee of the relevant Fund entity, and SAIL shall include a CDD summary report in such final proposal.

6.2. In addition to the assessment of the Borrowers' existing AML/CFT risk management practices, SAIL also takes due steps, with the support of the AA, to ensure each Borrower's ongoing compliance with the Fund's AML/CFT standards.

6.3. SAIL ensures that the respective financing documents shall include adequate provisions to ensure the Borrower's compliance or commitment to comply in all respects with all local and, where relevant, EU AML/CFT standards, laws 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 the Borrower acting in its own name and for its own account;

6.3.3. information undertaking on KYC, AML/CFT and similar procedures;

6.3.4. undertaking to comply with local and, where relevant, EU laws, regulations and standards regarding AML/CFT, prevention of prohibited conduct standards and regulations and the FATF standards and recommendations;

6.3.5. undertaking not to engage in prohibited conduct (including ML and TF);

6.3.6. undertaking to implement, maintain and comply with (i) internal procedures and controls satisfactory to the Fund as lender for the purpose of preventing the Borrower, the Fund or the relevant financing arrangement from 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. SAIL will also obtain confirmation regarding the valid execution of the relevant lending documentation by the Borrowers and other relevant contractual parties (such as the Guarantors), satisfaction of conditions precedent and any other documents required by the relevant lending documentation.

6.5. For each new Borrower, SAIL shall include, in the final proposals presented to the relevant Fund entity's investment committee, the following:

6.5.1. a section describing the applicable AML/CFT risk management checks and due diligence performed by the AA on the relevant Borrower; and

6.5.2. the main findings with respect to the relevant Borrower's AML/CFT policy or other applicable AML/CFT risk management procedures and processes.

6.6. At reasonable intervals, and where required by the AA, SAIL confirms the existence and, if applicable, the 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, such confirmation entails the review of the relevant corporate documents of the Borrower, comprising the articles of association (or similar documents), company register extract 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 its funds.

7.2. Periodic and event-driven reviews of CDD

7.2.1. The ODD on the Customers includes the obligation to verify and, where appropriate, to update, periodically in accordance with the applicable risk categorisation of the Customer, the documents, data or information gathered on the Customer and its UBO(s) while fulfilling the CDD obligations; *provided* that such documents, data and information shall be verified and updated immediately when a suspicion of ML/TF 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, changes to the composition of the Customer's management body and its authorised representatives and/or authorised signatories, media alerts, negative events, imposition of sanctions etc., which can also result in the 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 Management Body, with assistance from the AA and SAIL, will determine how the Fund can carefully phase out the business relationship with the Customer within a reasonable period of time. In the interim, adequate mitigating actions need to be taken, such as blocking any further disbursements or other payments 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	Normal	Enhanced
Monitoring frequency	Once every five (5) years	Once every three (3) 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 Fund 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 the suspicion and providing any and all relevant information. In the event that the unusual activity relates to the AMLCO, then the relevant employee and/or contractual third-party service provider shall notify the Management Body of the relevant Fund entity in lieu of the AMLCO (it being understood that, in the case of the BOD, only the members of the BOD other than the AMLCO shall be so notified).

8.2. The AMLCO shall, without delay, determine whether an investigation by the AMLCO is required, with the purpose and goal of the investigation being to identify and understand the background to the 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 parties involved in the transaction, though not with employees of the Customer.

8.3. If, after such investigation, 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 must determine whether or not an external report to FIU-Nederland is required based on all available information. Reports of unusual transactions to FIU-Nederland must be made by the AMLCO without delay and, in any event, within 14 days of the AMLCO becoming aware of the unusual nature of the relevant transaction.

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 any required additional investigations, whether or not the relevant transaction remains suspicious and must be reported to FIU-Nederland or whether there is some additional information that removes the suspicion.

8.5. All suspicions, whether reported to the AMLCO or identified by the AMLCO himself/herself and regardless of the ultimate action taken (or to be taken) by the AMLCO, must be submitted to the Management Body of the relevant Fund entity. All relevant documentation (including any report filed with FIU-Nederland and any document supporting the reasoning behind the ultimate decision taken by the AMLCO) must be kept on file by the AMLCO.

8.6. The AMLCO shall respond, quickly and comprehensively, to all information requests from the competent authorities (including, without limitation, the Dutch Central Bank (*De Nederlandsche Bank*) and FIU-Nederland) with regard to AML/CFT matters.

LIST OF ANNEXES

ANNEX 1: RISK-BASED APPROACH TO AML/CFT

ANNEX 2: TEMPLATE AML REPORT PROVIDED BY THE AA

ANNEX 3: TEMPLATE ANNUAL REPORT PROVIDED BY THE AMLCO

ANNEX 4: REGISTRATION OF BENEFICIAL OWNERS

ANNEX 5: KYC FOR CUSTOMERS

ANNEX 6: DEFINITIONS

+31 (0)70 744 8884
info@andgreen.fund
www.andgreen.fund

Basisweg 10, 1043AP
Amsterdam, The Netherlands

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 an 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 channelling 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 categorise a Customer as High risk even if none of the listed High risk factors apply. To the extent permitted by law, the AA may categorise a Customer as Medium or Low risk Customer even if one or more High risk factors apply, 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 the 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 EU list of high-risk third countries presenting strategic deficiencies in their AML/CFT regimes;
- Countries of higher risk as mentioned in the FATF's lists of 'High-Risk Jurisdictions Subject to a Call for Action' and 'Jurisdictions under Increased Monitoring';

- Countries on the EU and/or Dutch lists 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 United Nations, the EU or the United States of America (Office of Foreign Assets Control – OFAC);
- Countries with a high AML/CFT index, high corruption and/or high crime rates (as established by the Basel Institute on Governance or Transparency International).

1.2.3. The AA will regularly consult a range of relevant sources to assess 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 lists of 'High-Risk Jurisdictions Subject to a Call for Action' and 'Jurisdictions Under Increased Monitoring';
- the EU list of high-risk third countries presenting strategic deficiencies in their AML/CFT regimes;
- Transparency International (Corruption Perceptions Index);
- Basel AML Index annual reports issued by the Basel Institute on Governance.

1.3. <u>Customer-specific risk factors</u>

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 organisational 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 the 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 organised 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 recognised stock exchange in the EU, the United Kingdom ("**UK**"), the United States of America ("**US**"), New Zealand, Australia, Japan, Singapore, South Korea, South Africa, Switzerland or Israel;
- Non-listed entities that are a 100% (direct or indirect) subsidiary of a listed company on a recognised stock exchange;
- Government institutions or majority stated-owned enterprises from the EU, the European Economic Area or equivalent low-risk jurisdictions (UK, US, New Zealand, Australia, Japan, Singapore, South Korea, South Africa, Switzerland, Israel).

(The Contributors 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 Category

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 and verification of identity	✓	✓	✓
Database screening	✓	✓	✓
Extended research of other publicly available sources		✓	✓
Commissioning external background study[1]			✓
Assessment of the adequacy of the local AML/CFT regulatory framework based on the resources listed in **Clause 1.2.3** of this **Annex 1**	✓	✓	✓
Assessment of Customer ML/TF policies and procedures:			
Detailed/targeted questions on the Customer's AML/CFT risk management framework, organisation, structure and capacities prepared by SAIL and/or the AA		✓	✓
Additional off-site review of the Customer's relevant AML/CFT risk management policies and procedures and compliance & internal audit reports			✓
Additional on-site interviews with key credit, compliance and internal audit personnel of the Customer performed by SAIL			✓
Documentary due diligence			
Collection and verification of relevant corporate constitutional documents, licences and approvals as well as various identification documents and signing authorities (based on the level of CDD applied)	✓	✓	✓

3.1. SDD

During an SDD, the AA will collect a limited amount of AML/CFT information on the Customer, including (without limitation and as necessary or appropriate in respect of the relevant Customer) a list of authorised signatories and/or a statement confirming signatory authorisation, identification and verification of identity information for each UBO and each authorised signatory, information available on public registers and other public resources, an extract from the relevant register of commerce (or equivalent) and a copy of the Customer's regulatory licence(s) (if any).

3.2. EDD

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

[1] Commissioned only in specific cases, typically where specific ML/TF Red Flags point to a Higher risk profile.

3.2.2. The AA applies the following EDD procedure:

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

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 authorised 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 explicit AMLCO approval is a separate and mandatory step before the relevant (prospective) Customer is fully accepted by the AMLCO or the Management Body (as applicable).

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

- together with SAIL, request the Customer to provide copies of CDD documents that are used to verify the identity of the Customer, its UBO or authorised representative(s) that are certified as a true copy of the original 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, etc.)
  - 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 offences or involvement in ML/TF practices; and/or
  - questionable business practices in other ventures.

4. PEP Assessment

4.1. The definition of a PEP is set out in Annex 6.

4.2. The procedures to determine whether a Customer, its authorised representative or its 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 PEPs 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 stated-owned enterprises (each, an "**SOE**") from EU or equivalent low-risk jurisdictions. These are indicators of Low risk. However, at the level of the pseudo-UBOs or authorised representative(s) of such Contributors, certain persons are likely to qualify as PEPs, which triggers EDD.

4.3.3. If the sole reason for the PEP status is the identification of a person as pseudo-UBO or authorised representative of a government or SOE from a Low risk jurisdiction, then:

- after applying EDD; 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 PEPs will be Low as well.

+31 (0)70 744 8884
info@andgreen.fund
www.andgreen.fund

Basisweg 10, 1043AP
Amsterdam, The Netherlands

ANNEX 2: TEMPLATE AML REPORT PROVIDED BY THE AA

STICHTING ANDGREEN.FUND
&GREEN FUND B.V.
&GREEN FUND VEHICLE B.V.

(collectively, the "Fund")

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

To : AML/CFT Compliance Officer of the Fund ("**AMLCO**")

From : Intertrust (Netherlands) B.V. ("**AA**")

Date : [DATE]

This AML/CFT confirmation provided by the AA for the period [PERIOD] (the "**Period**"), to be appended to the AMCLO Report for the Period as Annex I thereof, confirms that:

- the Fund has delegated the CDD procedure for Customers to the AA;
- all Customers of the Fund have been identified in accordance with the Fund's AML/CFT policy;
- the number of Customers to whom Enhanced Customer Due Diligence (EDD) was applied in the Period was [number];
- the number of Customers to whom Normal Customer Due Diligence (NDD) was applied in the Period was [number];
- the number of Customers to whom Simplified Customer Due Diligence (SDD) was applied in the Period was [number];
- the number of unusual transactions/activities by Customers that were identified by the AA and reported to the AMLCO in the Period was: [number]; and
- the AA's AML/CFT operations comply with the applicable legal and regulatory provisions as regards the prevention of ML/TF and, in particular, the AA's personnel received adequate AML/CFT training for the implementation of the AML/CFT framework applicable to the Fund in the Period.

Customer	Relevant Fund Entity	Customer Type	Risk profile	Type of CDD/ ODD	Review frequency	Last review	Next periodic review

All defined terms used but not defined herein shall have the meaning given to such terms in the AML/CFT policy of the Fund.

[DATE]

Signature

+31 (0)70 744 8884
info@andgreen.fund
www.andgreen.fund

Basisweg 10, 1043AP
Amsterdam, The Netherlands

ANNEX 3: TEMPLATE ANNUAL REPORT PROVIDED BY THE AMLCO

STICHTING ANDGREEN.FUND
&GREEN FUND B.V.
&GREEN FUND VEHICLE B.V.

(collectively, the "Fund")

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

To : Members of the Management Body

From : [NAME] , AML/CFT Compliance Officer of the Fund ("**AMLCO**")

Date : [DATE]

Items related to AML/CFT matters to be brought to the attention of the Management Body: [●] / [N/A]

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

- all Customers of the Fund have been identified in accordance with the Fund's AML/CFT policy;
- the number of Customers to whom Enhanced Customer Due Diligence (EDD) was applied in the Period was [number];
- the number of Customers to whom Normal Customer Due Diligence (NDD) was applied in the Period was [number];
- the number of Customers to whom Simplified Customer Due Diligence (SDD) was applied in the Period was [number];
- the number of unusual transactions/activities by Customers that were identified by the AA and reported to the AMLCO in the Period was: [number]; and
- the AA's AML/CFT operations comply with the applicable legal and regulatory provisions as regards the prevention of ML/TF and, in particular, the AA's personnel received adequate AML/CFT training for the implementation of the AML/CFT framework applicable to the Fund in the Period.

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

- the detail and implementation of the AML/CFT framework applied by the AA;
- the level of professional knowledge and capacity of the AML/CFT team at the AA; and
- the AML/CFT training programme 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 and/or any identified unusual transactions have been appropriately dealt with in accordance with applicable AML/CFT laws and regulations;
- no report has been made to any competent authorities with respect to the AML/CFT aspects of the operations of the Fund or, if applicable, any such required report has been made in accordance with applicable AML/CFT laws and regulations; and
- he/she has dedicated sufficient time during the past year to keeping himself or herself up-to-date with the AML/CFT legal and regulatory requirements applicable to the Fund.

All defined terms used but not defined herein shall have the meaning given to such terms in the AML/CFT policy of the Fund.

[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(s) ("**UBO(s)**") 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 the AA and has agreed with the AA that any registration of a new UBO, or any change to UBO data, will be managed as follows:

- In connection with the first registration of a UBO, or any change to a UBO's data, the Fund, through SAIL, will inform the AA by means of a written communication containing at least the following mandatory information with respect to each UBO:
  - a) the name(s);
  - 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 stated on the relevant individual's identification document and/or passport in the event that the UBO is not residing in the Netherlands and consequently is not registered with the BRP; and
  - i) the type and extent of the beneficial interests held.
- The AA will check the UBO register to determine if the new UBO or the new UBO data has been registered by another party (such as the relevant notary, if applicable) and, if so, that the correct data has been registered.
- Where the new UBO, or the new UBO data, has not been registered, the AA will file the above-mentioned information, together with the required supporting documents (*i.e.*, identification document), with the UBO register within the required timeframe from the time when the Fund became aware of, or should have known, the event triggering the necessity of registration or modification of any UBO information.
- The AA will report back to the Fund by sending a copy of the proof of registration by e-mail to SAIL.
- The Fund, the AA and SAIL undertake to inform each other of any change in the structure or organisation of the Fund that could potentially lead to a change in the UBO(s) identified or in the data with respect to an existing UBO.

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

The Fund shall obtain, and keep at its registered office, current, accurate and constantly updated information on its UBO(s). 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 (such as banks and asset managers, among others) upon a reasonable request.

The Fund shall designate the place where the UBO information and supporting documents will be kept for a period of five years from the date on which the relevant registered entity was 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 of Customer	CDD requirements	Verification
Natural	• first name and surname • place and date of birth • nationality • address and country of residence • official national identification number / passport *(where available)*	• address verification • certified passport, ID or residence permit *(one valid official identification document issued by a public authority and which bears the Customer's signature and picture)*
Legal	• full legal 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 (certificate of incorporation, memorandum and articles of association or equivalent (as well as any amendments thereto)) • annual report and/or latest audited accounts *(if applicable)* • register of commerce or any equivalent document issued by a local public authority *(if applicable)* • operating licence *(if applicable)* • list of authorised signatories • statement confirming signatory authorisation • confirmation of good tax standing *(where available)* • FATCA/CRS self-certification • 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) • certified copies of passports and evidence of registered address of directors and UBOs of the legal entity • determine if acting for own account or on behalf of others	• address verification • current articles of association • confirmation of good tax standing *(where available)* • current extract from the company's shareholder/owner register or structure chart

Trust	• requirements for Legal **plus**:
	  ○ settlors' information (Natural / Legal)
	  ○ trustees' information (Natural / Legal)
	  ○ beneficiaries' information (Natural / Legal)
	  ○ protector information (Natural / Legal) *(if applicable)*
		• Requirements for Legal

Fund	• requirements for Legal **plus**:
	  ○ investors' information (Natural / Legal)
	  ○ fund manager's information (Natural / Legal)
		• Requirements for Legal

ANNEX 6: 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 centre countries of Europe, North and South America and Asia.

FATF list of high-risk and other monitored jurisdictions: Based on reviews conducted 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: "*High-Risk Jurisdictions subject to a Call for Action*" and "*Jurisdictions under Increased Monitoring*". These lists highlight countries requiring urgent countermeasures and, respectively, countries committed to addressing identified deficiencies under FATF monitoring.

Financing of Terrorism (*financieren van terrorisme*) (**FT**) means behaviour that is punishable pursuant to article 421(1) of the Dutch Penal Code (*Wetboek van strafrecht*). In essence, financing of terrorism occurs when assets are used to enable terrorist activities, whereas proliferation financing relates to funding activities connected to the production, acquisition, transportation, etc. of weapons of mass destruction.

Money Laundering (ML) means behaviour that is punishable pursuant to articles 420*bis*, 420*bis*.1, 420*ter*, 420*quater* and 420*quater*.1 of the Dutch Penal Code (*Wetboek van strafrecht*). In essence, money laundering means that illegally obtained assets are made legal, such that the illegal origin is no longer visible.

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, deputy or assistant ministers and State secretaries (*staatssecretarissen*)
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, constitutional courts or 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; and
- directors, deputy directors and members of the board or equivalent function of an international organisation.

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; and

- 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; and
- 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 shall be 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 organised crime and criminal activities of the Customer's UBO or of any member of its 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 with the Customer in question. Disclosure of actions by regulatory bodies, such as regulatory fines or sanctions against existing Customers, upon becoming aware thereof, must be brought to the attention of the Management Body of the relevant Fund entity.
- Business relationships with PEPs or with other high-risk Customers 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 Customers may be vulnerable in case of regime change.
- In addition to the principles described above, the Fund shall avoid entering into 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 AML/CFT regulatory framework, particularly the application of the recommendations made by the FATF and the level of compliance of the Customer's AML/CFT policies and controls with local and international standards. In the absence of a proper local AML/CFT 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 more than 25% 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 more than 25% 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; or
- if no natural person can be identified as an Ultimate Beneficial Owner in accordance with the above criteria, or if there is any doubt as to whether the identified persons are the UBOs, the natural person(s) acting as the senior managing official(s) of the corporate entity shall be identified as the UBO(s) of such corporate entity;

in the case of a partnership, a shipping company (*rederij*), 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 above is identified, the natural person(s) who are the partners (*vennoten*) of the partnership, excluding limited partners (*stille vennoten*); and

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; or
- any other natural person exercising ultimate control over the trust or the entity by means of direct or indirect ownership or by other means.