Contents

1. ABOUT CAPITAL 4 DEVELOPMENT ASIA FUND

Capital 4 Development Asia Fund Coöperatief U.A., is a fund incorporated under the laws of the Netherlands to make equity and debt investments in small and mid-sized companies in India, Philippines, Indonesia and neighbouring south and south-east Asian countries ("Target Countries") to achieve social and environmental impact and medium-long term capital appreciation ("**C4D**"). Capital 4 Development Partners B.V. has been appointed to act as the exclusive fund manager for C4D and has local presence in the Target Countries through regional teams.

2. INTRODUCTION

2.1. Scope of the Policy

There is growing concern in the global community with regard to money laundering, financing of terrorism and related activities. Global international organizations and countries across the world have enacted laws and implemented rules and regulations to address issues arising from Money Laundering.

Integrity is one of C4D's core values and it aims to be honest, sincere, prudent and reliable in all its actions. C4D's conduct focuses on respect, integrity, professionalism and sustainability in its relationships. This means no one will be excluded from financing services other than on grounds of morality and creditworthiness.

C4D is a strong supporter of anti-money laundering efforts. As part of this focus, C4D affirms that it shall only conduct business with companies, individuals and investors who have honest intentions and do not entail any risks for C4D. For this reason, C4D has identified and adopted anti-money laundering and due diligence processes which are based on the principle of "Know Your Customer". The basic principle of these processes is to collect and record as much information as possible in any situation which then provide a basis for customer acceptance and risk classification. These processes guide C4D in conducting effective customer integrity checks to detect a possible connection with financing of terrorism, Money Laundering and / or fraud, thereby preventing C4D from doing business with customers with dishonest or even criminal intentions. This Anti-Money Laundering and Customer Due Diligence Policy ("this Policy") lays down in detail the anti-money laundering and due diligence processes that C4D and its staff should follow and describes the minimum standards for adherence of such processes.

2.2. Recognised Risks

Reducing risks is one of the key objectives of performing the due diligence procedures set forth under this Policy. C4D being a fund, assets typically flow into the fund from other financial institutions which are themselves regulated for anti-money laundering purposes, which reduces the risk of Money Laundering. Despite this, C4D recognizes that, it is exposed to four types of risks on account of its business operations and practices:

- *Reputational Risk:* The risk of adverse publicity due to the involvement of C4D in the 'dealing and wheeling' of dishonest customers.
- *Operational Risk:* The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risks in the KYC context relate to ineffective control procedures and failure to practice due diligence.
- *Legal Risk:* The risk of law suits, criminal prosecution and the related fines, damage compensation and sanctions, as a consequence of insufficient knowledge or insight into the legal constructions 'behind the customer'.

- *Concentration Risk:* The risk of doing too much business with persons or enterprises that ultimately belong to the same conglomeration, due to not knowing precisely who the customers are, and their relationship with other customers.

2.3. Objectives

C4D aims for growth and sustainability. This calls for responsible action, transparency, risk management and a long-term vision. This Policy is an expression of these basic principles and supports C4D in developing sustainable relationships with reliable partners.

The objectives of this Policy are:
- To comply with Dutch, Target Countries' and International (as far as possible) financial sector guidelines on anti-Money Laundering, customer due diligence and KYC procedures;
- To lay down procedures for and set a standard for customer due diligence at C4D;
- To reduce C4D's exposure to operational risk, legal risk and concentration risk; and
- To prevent C4D from being involved in situations that may lead to integrity risk and therefore reputational damage.

2.4. Legal Framework

This Policy is based on the following laws and legislations:

- Dutch Prevention of Money Laundering and Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft): This act is based on the third European Union Anti-Money Laundering Directive, which is based on the Financial Action Task Force (FATF) recommendations.

- The Dutch Financial Supervision Act (Wet financieel toezicht – Wft): This act contains customer due diligence requirements designed to address reputation, operational, legal and concentration risk. It is based on 'The Customer Due Diligence for Banks Report' that was adopted by the Basel Committee on Banking Supervision in late 2001. C4D, as a separate legal entity without banking license, strictly seen is not subjected to Wft. Nevertheless, C4D choses to implement this act into this Policy to be seen as a reliable and professional business partner by all our stakeholders.

3. DEFINITIONS

Authorised Signatory(ies)	*Any person who is authorized to act on behalf of the Customer holding a valid power of attorney or document giving the person power to act on behalf of the Customer.*
Background Checks	*Perform a check against the applicable sanctions lists, PEP list, screen for adverse information and check, if applicable, internal warning system or internal list.*
Certification	*Certification of a copy of an original document means signing and dating the copy with the words 'original seen by' followed by the name, position and contact details of the person carrying out the certification. When the document includes a copy of a photograph, 'true likeness' must be written on the copy.*
Certified True Copy	*A declaration derived from a Qualified Source or made by a Qualified Party stating that the copy was made from the original.*
Close Associates	*A person is said to be close associate of another person if they are closely connected to such person, socially or professionally and shall include:*

	1. *any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with such person;* 2. *any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of such person.*
Compliance Officer	*An individual designated by C4D to fulfil all compliance activities under this Policy.*
Customer	*A natural person or legal entity with whom a business relationship is established or for whom a transaction is carried out or is proposed to be established or carried out. For C4D, Customer includes its:* *1. investors and prospective investors,* *2. the purchasers of an investment held by C4D and its management; and* *3. investees and potential investees and their existing management, directors and shareholders.*
Customer Due Diligence (CDD)	*The set of policies, measures and procedures in place to identify, assess and control the risks to C4D inherent in executing services for Customers. By executing CDD, C4D is able to prevent or detect a possible connection with Financing of Terrorism, Money Laundering and/or fraud and keep off customers with dishonest or even criminal intentions.*
Customer Integrity Risk	*The risk that a (potential) Customer of C4D is involved in dishonest or criminal activities.*
Customer Owner(s)	*Subject to the below exception, Customer Owner shall refer to each of the investment managers of the regional teams of the Fund Manager based in the Target Countries;* *In cases where the Customer is an investor or prospective investor in C4D, Customer Owner shall mean the Compliance Officer, except where the Compliance Officer delegates this function to an investment manager of a regional team of the Fund Manager or any member of the Fund Management Team, the Customer Owner shall be such person.*
Family Members	*Family members shall include the following:* 1. *the spouse;* 2. *any partner considered by national law as equivalent to the spouse;* *3. the children and their spouses or partners; and* *4. the parents*
Fund Manager	*Will mean Capital 4 Development Partners B.V.*
Fund Management Team	*Shall mean all the employees, consultants and advisors of the Fund Manager and all the legal entities incorporated by or under it, in the Target Countries with the intention of effective management of the regional portfolio.*
Know Your Customer (KYC)	*Refers to the measures and procedures in place to determine with whom a relation has or will be established and to ascertain relevant information pertinent to doing financial business with them.*

Material Adverse Information	*Shall mean publicly available information of the last 2 years noting a possible involvement of the Customer or any of the Customer's officers, directors, Authorized Signatories or UBOs in:* *1. Money Laundering or Terrorist Financing activities.* *2. Other criminal or fraudulent activity related to or in connection with the business operations or activities of the Customer.* *3. Other criminal or fraudulent activity that is not related to or in connection with the business operations or activities of the customer, but is significant enough that it can impact the reputation of C4D.*
Money Laundering	*Money laundering is defined as changing money and / or valuables obtained from criminal activities into seemingly legitimate funds with the aim of concealing their criminal origins and reintroducing these funds to make them appear legitimate.*
Non-governmental organisation (NGO)	*A non-governmental organisation (NGO) is a legally constituted organization created by natural or legal persons that operates independently from any government. In the cases in which NGOs are funded totally or partially by governments, the NGO maintains its non-governmental status by excluding government representatives from membership in the organization. The term is usually applied only to organizations that pursue some wider social aim that has political aspects, but that are not overtly political organizations such as political parties.*
Politically Exposed Person (PEP)	*PEPs are natural persons who are or have been entrusted with prominent public functions.* *Natural persons who are or have been entrusted with prominent public functions shall include the following:* *(a) heads of State, heads of government, ministers and deputy or assistant ministers;* *(b) members of parliaments;* *(c) members of supreme courts, of constitutional courts or of other high- level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;* *(d) members of courts of auditors or of the boards of central banks;* *(e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;* *(f) members of the administrative, management or supervisory bodies of State-owned enterprises.* *None of the categories set out in points (a) to (f) shall be understood as covering middle ranking or more junior officials. The categories set out in points (a) to (e) shall, where applicable, include positions at the community and international level.*
Qualified Party	*A government appointed official or professional, subject to some form of official disciplinary rules, such as:* *1. An embassy, consulate of high commission;* *2. A lawyer, attorney or notary (independent, not an employee of the customer); or* *3. Another (government) appointed official or professional subject to some form of official disciplinary rules*
Qualified Sources	*Qualified sources are:* *1. Website of the Customer's regulator;* *2. Online connection with Chamber of Commerce or other company house register;* *3. Audited financial statements;* *4. Company document certified by a Qualified Party; and*

	5. *Other (electronic) means to access information with an undisputed integrity, such as Dun & Bradstreet, Lexis Nexis*
Sanction Country	*A country which is subject to Sanctions.*
Sanctions	*Means any economic or financial measures, or trade embargoes or restrictive measures, implemented, administered or enforced by European Union, Dutch government or local authorities of Target Countries or the Countries in which the Customer resides, including through rules, regulations or directives, and any executive orders imposing economic or financial sanctions on any individuals, entities or foreign countries or regimes.*
Source of Funds	*The origins of the funds and/or assets used in the business relationship with C4D.*
Terrorist Financing	*Deliberate acquisition, possession or provision of objects with a monetary value intended for committing a terroristic crime (as referred to in Section 83 of the Dutch Criminal Code). And the provision of financial support, as well as deliberate fundraising in aid of an organization of which the object is to commit terroristic crimes (as referred to in Section 83 of the Dutch Criminal Code).*
Ultimate Beneficial Owner (UBO)	*'Beneficial owner' means the natural person(s) who ultimately owns or controls the Customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall include:* *(a) in the case of corporate entities:* *(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity; a percentage of 25% shall be deemed sufficient to meet this criterion;* *(ii) the natural person(s) who otherwise exercises control over the management of a legal entity.* *(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:* *(i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of ≥25% of the property of a legal arrangement or entity;* *(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;* *(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity.* *Following this definition, most cooperatives will not have UBOs, unless one of the members of the cooperative has over 25% of the voting rights in the cooperative.*

4. ROLES AND RESPONSIBILITIES

4.1. Management

The Fund Manager shall govern C4D Asia Fund's compliance with this Policy. The responsibilities of the Fund Manager are listed below:

- Decide on measures to be taken in case Customers are rated as “High Risk” or “Unacceptable Risk”;
- Verify effectiveness of the measures that have been taken in relation to Customers rated as “High Risk” or “Unacceptable Risk”;
- Decide on accepting and reviewing Customers that are situated in a Sanction Country;
- Decide on accepting Customers in (complex) cases presented by the Compliance Officer and Customer Owners and also whether such acceptance will be on an ad-hoc basis or continual basis;
- Training and development for the Compliance Officer, Fund Management Team and the Customer Owners for the subject matter of this Policy; and
- Take measures to mitigate the occurrence of any atypical situations or suspicious transactions in regards to the subject matter of this Policy.

4.2. **Compliance Officer:**

The managing partner of the Fund Manager will be designated as the Compliance Officer under this Policy. A representative of the Fund Manager, the Compliance Officer will be the link between the Fund Manager and the Customer Owner. The responsibilities of the Compliance Officer are as follows:

- Where the Customer is an investor or prospective investor in C4D, CDD processes will be carried out primarily by the Compliance Officer unless delegated to an investment manager of a regional team of the Fund Manager or member from the Fund Management Team;
- Ensure that this Policy in compliance with all applicable anti-Money Laundering, KYC and customer due diligence legislation, regulation and group guidelines and update the same from time to time;
- Monitor and supervise the operational execution and implementation of this Policy by the Fund Management Team;
- Ensure that this Policy is translated into effective operational guidelines, procedures and work instructions and make sure that all employees, consultants and advisors are effectively trained to execute and implement this Policy;
- Discuss with the Customer Owner and monitor Customers with a Money Laundering risk indication;
- Assign a risk rating to the Customer based on the outcome of the CDD and the recommendations of the Customer Owner;
- Ensure that there is groupwide adherence to this Policy;
- Oversee C4D’s anti-Money Laundering systems and manage of C4D’s Money Laundering risks and highlight to the Fund Manager in case of any revisions would be required; and
- Review the outcomes of the CDD and necessary documentation and provide a sign off that he/she is satisfied with the checks undertaken and that they indicate no evidence of Money Laundering. This is to be done just before an investment or transaction is signed off, an investor is accepted to C4D or an investment is sold.

4.3. **Customer Owner**

Where the Customer is a purchaser of an investment held by C4D or is an investee or a potential investee of C4D, CDD processes will be carried out by the investment manager (or the Customer Owner) of that regional team where the investee or the investment held is located. Each such Customer shall have a single Customer Owner within C4D, who will be the single point of contact for all CDD inquiries, additional documentation. The responsibilities of the Customer Owner shall include:

- The Customer Owner will process the Customers’ investment application, internally and externally and will create and maintain a file for each Customer under his responsibility (“CDD File”). The Customer Owner will ensure that evidencing documentation will be kept available at all times in the CDD File.
- The Customer Owner will also sign-off on the CDD of a Customer before forwarding the CDD File to the Compliance Officer for records and reference; and

- It is the responsibility of the Customer Owner to monitor and supervise Customer Integrity Risk and timely escalate to the Compliance Officer signals that could potentially lead a deterioration of the risk classification of a Customer.

Certain CDD tasks may be delegated to support officers (e.g. internal account managers / back office) from within the Fund Management Team. However, the overall Customer responsibility cannot be delegated and remains the responsibility of the Customer Owner.

5. DUE DILIGENCE REQUIREMENTS

CDD has to be performed for every prospective and existing Customer by either the Customer Owner or the Compliance Officer as highlighted in Clauses 4.2 and 4.3. No business relations will be established or transactions will be executed for a Customer if the CDD requirements and processes are not fulfilled (including receipt of all required verification documentation).

The process of CDD begins with gathering information about the Customer and its UBOs, directors and Authorized Signatories, collecting documentary to verify the Customer's identity and culminates in assessing the Money Laundering and Terrorist Financing risks associated with that Customer in accordance with the below Clauses. The acquired information consists both of 'hard' data (e.g. identification documents, background checks) and 'soft' data (e.g. customer visit report, project information). The CDD also includes a proper plan to mitigate risks for Customers classified as "High-Risk" and "Unacceptable".

6. WHEN SHOULD THE DUE DILIGENCE BE CONDUCTED?

CDD processes should be completed along with obtaining of evidence at the following times:

- Fund Raising: Before the admission or acceptance of a new investor to C4D; and
- Investment and exit: When it is reasonably certain that a deal will be successfully completed but before the Fund Manager becomes legally obliged to complete an investment. In case of a new investment, the CDD process can form part of the due diligence processes performed by the Fund Manager on the proposed investee. Where there are subsequent changes to the board of directors, consideration should be given to the need to verify the identity of the new directors or shareholders before the changes takes place.

Depending on the risk classification of a Customer, the Customer Owner or the Compliance Officer, as the case may be, will be required to complete periodic CDD reviews, when requested for by the Fund Manager. In the event, new information is discovered or found concerning the Customer, a review will be initiated, depending on the nature of information discovered and the risk classification of the Customer. Please refer to Clause 11 of this Policy for more details on periodicity of CDD reviews.

7. DETERMINING CUSTOMER INTEGRITY

The goal of the CDD process is to identify the UBO or on whose behalf a transaction is made, by obtaining and collecting sufficient information about the potential Customer. Further, the Customer Owner or the Compliance Officer, as the case may be, should be able to identify at the outset, the intended nature of the relationship that the Customer will have with C4D. These are done in order to identify and evaluate any potential integrity and reputation risk to C4D by its associated with each Customer, before any business or transactions are undertaken between C4D and such Customer. The guiding principle for C4D is that, it only wishes to do business with Customers that it actually knows, who have honest intentions and that do not entail any unacceptable risks.

C4D's presence and work in rural areas of developing countries complicates the determination of customer integrity, particularly with limited availability of information. Therefore, C4D chooses to carry out the CDD process on the principle of "comply or explain". The Compliance Officer will formulate and adopt a check-list for each type of transaction, which should set the checks to be undertaken on the Customer and various parties to a transaction.

When it has been concluded that C4D cannot and should not engage into business with the Customer, the Customer must not be accepted, and for an existing Customer an exit process should be initiated at the earliest.

7.1. Identification

Identification is the process of providing a set of attributes which together uniquely distinguishes one private individual or (legal) entity from another. The documents and checks required to identify and verify the identity differ depending upon the nature of the person. Below is the list of minimum information that must be collected from (prospective) Customers and the documentation that can be collected against the same. The below list is by no means comprehensive and can be extended with additional documents to be called for, where deemed necessary. However, in no circumstance should the below list be shortened. The nature of service or transaction proposed to take place between the Customer and C4D should also be identified and recorded.

(a) Identification of organizations: The following information and documents should be collected from Customers that are not natural persons:

<table>
<tr><th>Information</th><th>Documentation</th></tr>
<tr><td>The full legal name and the trading name (if any) of the Customer</td><td rowspan="2">Memorandum and articles of association or the local equivalents / Partnership Deed / Trust Deed / any other constitutional documents.</td></tr>
<tr><td>Industry / Sector</td></tr>
<tr><td>The Customer's principal places of business, local offices and other physical locations</td><td>Declaration from the Customer certifying the places of business.</td></tr>
<tr><td>Country of incorporation</td><td rowspan="4">Certificate of Incorporation of any other legal registration documentation</td></tr>
<tr><td>Chamber of commerce number or equivalent, if applicable or existing</td></tr>
<tr><td>Customer entity type, e.g. cooperative, partnership, NGO, private legal company, etc.</td></tr>
<tr><td>The Customer's statutory (registered office) address</td></tr>
<tr><td>Information pertaining to the ownership and supervisory structure of the organization</td><td>- Ownership structure and structure chart as explained in Clause 7.4 below;
- directors and shareholders registers or the local equivalents;
- Identity of the partners owning more than 25% of the Customer.</td></tr>
</table>

If there is a reputable local company register or government records with information available to the public then a company search may provide this information.

(b) Identification of natural persons: Identification of a natural person (in the context of this Policy) refers to the identification of the Ultimate Beneficial Owners (UBO's), directors and Authorized Signatories of the Customer. The name, date of birth and residence details should be collected from Customers who are natural persons and from the UBOs, directors and Authorized Signatories. Photo identity documentation that verifies the name, date of birth, nationality, residence and in general, the identity of the individual should be collected for verification. The passport or any other government issued document with a picture of the individual – e.g. a driving licence or identity card are examples of the documentation that can be collected. If the above documents do not contain the residential address of the person, a recent utility bill or bank statement (less than three months old) showing both name and address is required. Similarly, in case the documents mentioned above do not mention the date of birth of the individual, other appropriate government issued documentation should be collected which mentions the date of birth. The names and addresses on the documentation should match what is known and declared of the individual.

7.2 Verification

Verification is the process of proving, through independent sources, the validity of the documentation collected as part of the CDD process and the correctness of the information by which the Customer is identified. The Customer Owner will be responsible for obtaining the appropriate verification documentation as set forth above and taking reasonable steps to verify the same. Appropriate verification methodologies may include documentary (as explained in detail below) or non-documentary (e.g. electronic database screening) methods and/or include cross-checks to verify information via public databases or other reliable sources (e.g. ensuring that tax identification or social security number information is valid and corresponds to the Customer). Appropriate verification methodologies may also include checking that funds are received from an account held in the name of the Customer with an appropriately regulated financial institution.

Documentation evidencing the correctness of information will be maintained as part of the CDD File for each Customer, after Certification by the Customer Owner.

(a) Documentary verification

Documentary verification is the method to verify the authenticity of the documents collected as part of the verification process. The quality of all copies of verification documents (including passports) should be such that the relevant information can be read. If there has been no face to face contact with the Customer *and* the information about the Customer indicates to a higher integrity risk, Certified True Copy should be obtained. Copies of Certified True Copies are not acceptable as part of the CDD process. In other cases, the documents collected should either be self-attested by the Customer itself or by the Authorized Signatory of the Customer. If there is a reputable local company register or government records with information available to the public then a company search may be used to verify the documents collected from the Customer.

To the extent a document used to verify a Customer's identification has an expiration date or set validity period (such as a passport or an identity card), the document must be valid for at least 3 months following the date on which it was accepted and relied upon as verification of the Customer's identification. In cases where the Customer Owner does not perceive the Customer to be of "High Risk", the documents which expire within 3 months may be admissible provided that the new, renewed and valid (copies of the) documents will be obtained and added to the Customer's CDD File as soon as they come available, subject to the approval of the Compliance Officer.

All documents obtained as part of the CDD process shall, once verified and confirmed that such documents are valid, legitimate and complete, be signed off by the Customer Owner or the Compliance Owner, as the case may be, prior to being added to the Customer's CDD file.

7.3 Onsite Customer Visit

Customer information is, due to the nature of C4D projects, often difficult to obtain. The onsite Customer visit is, therefore, an important source for obtaining and verifying CDD information, and monitoring organizational changes. The Compliance Officer may call for an onsite customer visit to be conducted by the Customer Owner, in cases where it deems the same necessary. If the Customer Owner delegates the Customer visit to a third party, it is the responsibility of the Customer Owner to clearly instruct this third party regarding the CDD process and relevant CDD signals. Soft information pertaining to the Customer and its UBOs, directors and Authorized Signatories can be collected during the visit.

7.4 Organizational Structure

(a) Ownership Structure and UBOs:

In order to identify the shareholder structure and the UBOs of the customer, the ownership chain should be followed until the ultimate beneficial owner or owners are identified as individuals.

Any documentation obtained supporting the ownership chain and UBOs should be included in the CDD File. In general, ownership information can be obtained directly from the Customer or from a chamber of commerce extract, can be found on the customer website or identified in audited annual reports or financial statements. If the Customer refuses to provide information on its UBOs this could be a reason to classify the customer as "High Risk" or even end the relationship with an existing Customer. For each UBO, independent of entity type, the information in accordance with Clause 7.1(b) must be captured and appropriate documentation verifying such information should be collected.

(b) Authorized Signatories

In cases of an Authorized Signatory, a valid power of attorney (original or copy which is certified true by the Customer) or an official document providing power to transact on behalf of the Customer, such as a resolution, must be obtained, in addition to the documentation as set forth under Clause 7.1 (b). Authorized signatories must be identified and verified and background checks need to be performed. Specimen signature of the Authorized Signatory certified by the Customer is also to be collected. If the Customer refuses to provide information on its Authorized Signatories, this could be a reason to classify the Customer as "High Risk" or even end the relationship with an existing Customer. The Customer Owner will ensure that the signatures across all documents and identification documents of the respective parties to the transaction match with each other.

7.5 Background Checks

Background checks need to be conducted on the Customer and, when identified, on the UBOs, Authorized Signatories and directors as well. Background checks will include:

- PEP checks
- Sanction checks
- Adverse information checks

(a) PEP:

A potential risk associated with PEPs is that the Source of Funds, wealth or income may be from corruption. PEPs entail a higher risk from a Money Laundering or Terrorist Financing perspective and may present additional risks if they have control or influence over state-owned government or corporate accounts. PEP checks are performed on individuals. Since C4D does not, in general, have individual

customers, PEP checks are conducted on individuals associated with the Customers, such as UBOs, directors and Authorized Signatories. The results of the checks, (even if no match is generated), will be included in the CDD File. In case of false-positives, an explanation will be included as to why the alert is in fact not a match (e.g. date of birth, occupation or country of individuals involved being researched does not match). If the Customer by itself is not a PEP, but is identified as a Family Member or Close Associate of a PEP, then the PEP check requirements should apply to such Customer accordingly.

If it is concluded that a Customer is or the Family Member of Close Associate of such Customer is a PEP, the Customer Owner will inform the Compliance Officer and the Fund Manager will determine if the Customer can still be accepted. If the Customer is accepted, it will be initially classified as "High Risk".

For all accounts where either the Customer itself or a UBO of the Customer is identified as a PEP or a Family Member or Close Associate of the Customer is identified as a PEP, the Source of Funds, income, wealth and assets needs to be identified. Information can be obtained from public internet searches or directly from the Customer. A Customer's Source of Funds can also be evidenced from the statements of accounts provided. Where doubts still exit, the Customer Owner or the Compliance Officer may call for additional information such as the additional years of bank statements, tax filings, etc. All information collected must be reasonable and consistent, and must be documented and maintained in the CDD File by the Customer Owner. Further, the Fund Manager should review Customers who classify as PEP and consider an enhanced due diligence, where necessary. Where enhanced CDD cannot be performed, no transaction with such Customer should be undertaken.

(b) Sanctions:

All Customers should be screened against the lists of restricted entities and individuals imposed by the Dutch government through the United Nations or the European Union and local regulators of the countries in which the Customer resides, to ensure that Customers and their UBOs, directors and Authorized Signatories do not appear on a sanctions list. The results of the checks, also if no match is generated, will be included in the CDD File. The lowest risk level that Customers that are established in a Sanction Country will be "Medium Risk", however, this will be subject to change depending on the outcomes of the CDD process.

(c) Adverse Information:

As part of the CDD process, Customer Owners are required to perform news screening for all Customers to determine if any Material Adverse Information is available or published on the Customer or any other related parties identified during CDD as associated with the Customer. Public news sources such as Factiva Dow Jones and Google should be consulted to check if the Customer, and when identified, the UBOs, directors and Authorized Signatories of the Customer appear in the press negatively. It must be judged, if engaging into or continuing the relation could impact the reputation of C4D and/or its investors and stakeholders negatively.

If Material Adverse Information is found it must be documented by the Customer Owner and the Fund Manager should determine whether or not the Customer can be accepted or if the - already existing - relationship can be continued by C4D. If Material Adverse Information is found, but it is determined to be immaterial, then the rationale for this decision should be documented, and the Compliance Officer should be kept informed. The findings of the search, whether Material Adverse Information is found or not, should be included in the Customer's CDD File.

8. ANTI-MONEY LAUNDERING:

By engaging in Money Laundering, criminals aim to avoid that the money from underlying criminal activities come to the attention of regulatory authorities. Disciplinary measures will be taken against employees who participate in Money Laundering or that consciously fail to report unusual transactions.

The presence of C4D in countries that are classified as being more susceptible to Money Laundering asks for additional vigilance. ING accounts are used for the financial transactions of C4D. As part of ING's internal compliance and processes, ING monitored its accounts, which reduces the risk of Money Laundering involvement Customer visits and regular customer contacts serve as an opportunity to assess Money Laundering risks. Customer Owners are required to vigilant and identify any red flags that point towards Money Laundering activities and take appropriate measures thereafter. Examples of red flags for suspicious activity of Money Laundering and mitigating measures can be found below.

Red Flags	**Indicators**	**Mitigating measures**
Unusual activity without economic purpose	Despite clear requests, the Customer is not able to logically explain partnerships and transactions	Escalate to the Compliance Officer, who will escalate to the Fund Manager
Loan repayment to / from unrelated third parties	- Identify instances where a loan repayment has been made by a party other than the borrower (or importer in case of Sales Right agreement) - Customer wishes to use cheques drawn on an account other than their own or to have funds due to them paid into an account that is not their own.	Identify third parties, check integrity, ask Customer for an explanation and keep the Compliance Officer.
Loan repayment	- Identify if repayment of the loan or past loans is not according to the agreed schedule. - Changes in settlement and repayment details at the last moment, without a satisfactory explanation.	Check with the Customer
Unusual economic activity for the Customer	- Customer is trading products which are not according to their customer profile (either based on transaction history or CDD information) - Customers whose investment and lifestyle appear to be unrelated to their occupation - Customers whose proposed investment or proposed business relationship with C4D does not appear to match their occupation or their income levels.	Check with the Customer and escalate to the Compliance Officer, who will escalate to the Fund Manager.

Repayment before the scheduled/agreed term or early repayment in one amount	Identify if repayment of the loan is not according to the agreed schedule	Check with the Customer
Difficulty in verification of identification	- Reluctance in Customers to provide identification details for verification - Customers for whom verification of identity proves difficult.	Escalate to the Compliance Officer.

If no satisfactory explanation for an incident is obtained from the Customer, the Customer Owner is obliged to escalate the issue to the Compliance Officer, who will then decide on further measures.

9. RISK CLASSIFICATION AND CUSTOMER ACCEPTANCE

C4D is by nature active in countries that are qualified as being more susceptible to fraud, Money Laundering and/or other illegal activities. It is accepted that in these countries there is limited availability of information due to the level of organization of C4D's Customers and/or the jurisdiction in which the Customers operate. As a consequence, accepting (and reviewing) a Customer is based on the maximum amount of CDD information that could be acquired in a particular situation.

After the completion of the CDD or a CDD review, the risk qualification will be made by the Compliance Officer, based on the recommendation of the Customer Owner and the outcome of the CDD. C4D distinguishes between Low, Medium, High and Unacceptable Risk Customers.

Accepting a Customer and doing (further) business with such Customer, after the risk classification, is a decision of the Fund Manager.

9.1 "Low" or "Medium Risk" Customer

A Customer is to be classified as "Low Risk" where its (and its UBOs, directors and Authorized Representatives) identities and sources of wealth can be easily identified. A Customer is to be classified as "Medium Risk" where they are likely to pose a higher risk to C4D than an average "Low Risk" Customer.

9.2 "High-Risk" Customer

After the completion of the CDD, doubts might remain about (the intentions of) the Customer. The Customer Owner is required to inform the Fund Manager. A Customer is to be classified as a "High Risk" Customer if it is engaged in a profession, resides in a Sanction Country or presents a situation where the money-laundering risk is higher than normal. For example, Customers who have unnecessarily complex or opaque beneficial ownership structures can be classified as "High Risk". PEPs and Customers who refuse to provide information on their UBOs, directors or authorized signatories are to be classified as "High Risk".

Accepting a Customer that is qualified as being High-Risk (integrity risk) is permitted, as long as the reason for Customer acceptance is clearly explained and documented and measures have been taken to mitigate risks.

9.3 "Unacceptable Risk" Customer

After the completion of the CDD process it may become clear that the (integrity) risks to C4D regarding the potential Customer are unacceptable. Such Customers are to be classified as "Unacceptable Risk". Doing business or transacting with a Customer that is qualified as posing "Unacceptable Risk" is not permitted.

Measures in case of an "Unacceptable Risk" Customer: If the review of a Customer leads to a risk qualification of "Unacceptable Risk", the Fund Manager should identify measures to end the relationship with the Customer. The Fund Manager will also decide on the terms on which these measures must be taken and the Customer Owner will then implement and execute the same.

10. CUSTOMER DUE DILIGENCE REVIEW:

Certain Customers must be reviewed on a periodic basis. Similar to the acceptance of Customers, a CDD review is ruled by the principle "comply or explain". CDD reviews are conducted to assess whether the Customer's risk rating is still justified, whether documentation is still up to date, and whether there are any other findings that could pose a risk to C4D. The Compliance Officer and Customer Owner is responsible for ensuring that CDD reviews are conducted on a timely basis in accordance with the following timelines:

10.1 Periodicity:

(a) Periodic Review:

Depending on the risk rating assigned to the Customer and where the Compliance Officer suspects that the review of a Customer could potentially change the risk classification of the Customer, the Compliance Officer shall have the right to call for a fresh review of the Customer. The Compliance Officer shall use good professional judgement based on risk-sensitivity of the Customer for this.

The *recommended* timeline for the Compliance Officer to call for periodic reviews of Customers is indicated below:

- For "High-Risk" Customers, at least every 12 months;
- For "Medium Risk" Customers established in a Sanction Country at least every 18 months;
- For "Medium Risk" Customers not established in the Netherlands, at least every 30 months; and
- For "Medium Risk" Customers established in the Netherlands, at least every 42 months.

The Compliance Officer and/or the Customer Owner shall procure, on an annual basis, a declaration from each existing Customer confirming that there is no change in the status of the Customer, including but not limited to changes in the UBO, directors, etc. and that the information as collected at the time of the initial customer due diligence review is valid and remains unexpired and recognized as on the date of such declaration.

(b) Event driven review: An event driven review should be initiated if new information regarding a Customer is discovered (this is outside of the periodic review process). The Customer Owner is responsible for the event-driven review, after the same is approved by the Compliance Officer. An event driven review should at least take place in the following circumstances:
- Changes in UBO / directors / Authorized Signatories;
- Discovery of information regarding PEPs linked to the Customer that were previously unknown;
- Discovery of Material Adverse Information; or
- Other information (e.g. collected during a customer visit) that could lead to changes in Customer risk rating (country of incorporation, industry or sector, entity type)

10.2 Review Requirements:

CDD reviews, whether it is periodic or event driven, should be performed for Customers. Reviewing of Customers is the responsibility of the Customer Owner and must be documented. The review process to be

followed will be similar to conducting an CDD and the following should be checked and documentary evidence gathered:

- Any changes in name and address, Customer entity type;
- If the information regarding UBOs, Authorized Signatories and directors is still accurate;
- Performing new background checks (PEP, sanctions, adverse) on the Customer and its directors, UBOs and Authorized Signatories;
- Screening the Customer against the applicable Sanctions guidelines; and
- If the earlier decided measures to mitigate risks are adequately fulfilled.

If conflicting or new information is found, the Customer Owner should contact the Customer to obtain up-to-date verification information and documentation and update the CDD File accordingly. If Customers are no longer active (and have no outstanding transactions) and has exited, the CDD File should be closed with status marked as inactive. In such an event, a CDD review is not required. Should an inactive CDD File be re-opened on account of renewal of the business relationship, an immediate review of the Customer should be initiated to determine if additional CDD is required.

11. RECORD KEEPING, REPORTING AND TRAINING

11.1 Recordkeeping:

All CDD records must be kept for at least 5 (five) years from the closing of the account or completion of the transaction. The records should be held in a fire proof local data repository, either electronically or physically. All verification documentation, forms and the result of background checks must be stored in the CDD File. The CDD file along with the annual declarations, as set forth under clause 10.1(a), and the due diligence checklist signed off by the Customer Owner or the Compliance Officer, as the case maybe, shall be maintained on the cloud storage used by the C4D Asia Fund.

The Compliance Officer and the Fund Manager should at all time have access to records evidencing CDD. Legitimate requests for information, both internal and external, must be dealt with satisfactorily within a reasonable timeframe.

11.2 Reporting:

Information on the number and status of CDD Files should be readily available, when requested for by the Compliance Officer or the Fund Manager. The Compliance Officer will ensure that all reporting requirements under any applicable law with respect to the subject matter of this Policy is completed in a timely manner.

11.3 Training

The Fund Manager must ensure that staff responsible for CDD is adequately trained. Training is an ongoing process that is updated regularly to reflect current developments in and changes to laws and regulations, Money Laundering and Terrorist Financing trends and developments, as well as to reinforce internal policies and procedures.