Compliance Policy

Stichting Clean Energy and Energy Inclusion for Africa

(CEI Africa)

Adopted by the Board of CEI Africa on July 12th 2022
Approved by the Supervisory Council of CEI Africa on July 21st 2022

Version Control

Document history		
Version No	Date	Description / amendments
1	25-7-2022	To be shared with KfW for no-objection

1. Objective

The prevention and reduction of financial crime is a critical achievement that organisations must keep at the heart of the way they operate, of their decision-making process, and of their culture. Stichting Clean Energy and Energy Inclusion for Africa (**CEI Africa** or **'the Foundation'**) is committed to promoting and maintaining the highest professional standards and principles of integrity and conduct in all the aspects of the business it operates. This includes a customer on-boarding framework, and obligations in relation to anti money laundering and counter terrorist financing. CEI Africa is committed to take all appropriate and reasonable measures to mitigate against financial crime and its widespread impacts. One of these measures, is the establishment of a policy for entering into and handling relations with different parties. The primary goal of this Compliance Policy (**this Policy**) is guaranteeing that CEI Africa conducts identification, verification and (if applicable) acceptance of customers and other parties in an adequate and uniform way, in compliance with legal obligations as well as with international guidelines and best practices in the industry. This is to ensure that the process of fundraising for, investments by, lending by, guarantees by and grant making by CEI Africa is transparent and effective in preventing CEI Africa from being exposed to reputational damage or financial loss for non-compliance with relevant regulatory standards.

2. Scope

The scope of this Policy covers the following:

- Description of roles and responsibilities in relation to customer due diligence (CDD) and operational due diligence (ODD) in investments, lending, guarantees and grant making, whether within CEI Africa or with external parties (i.e., the Administrative Services Provider or ASP, etc.)
- The CDD and ODD process
- The on-going monitoring process

This Policy applies to all parties involved in the CDD and ODD processes.

Annex 1 to this Policy covers the due diligence framework in relation to Service Providers.

In drafting this Policy, international guidelines and good practices have been considered, such as:

- FATF Recommendations and findings concerning the approach to money laundering prevention in particular countries or jurisdictions.
- Wolfsberg Group Principles for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing.

3. Definitions and terms

AML	Anti-money laundering or any measures taken to prevent criminals from disguising funds illegally obtained (e.g., derived from or obtained, directly or indirectly, through the commission of a crime) as having a legitimate origin. This also includes the detection and reporting to relevant authorities of money laundering related suspicions.
ASP	The Administrative Service Provider, which is IQEQ and has been delegated certain operational compliance related duties and tasks

Board	The management Board of the Foundation, responsible for the general affairs of CEI Africa as well as the realization of the Foundation objectives.
CDD	Customer Due Diligence
Coercive practice	The impairing or harming, or threatening to impair or harm, directly or indirectly, any person or the property of the person with a view to influencing improperly the actions of a person.
Collusive practice	Arrangement between two or more persons designed to achieve an improper purpose, including to influence improperly the actions of another person.
Corruption and Corruptive practice or Corrupt Practice	The promising, offering, giving, making, insisting on, receiving, accepting or soliciting, directly or indirectly, of any illegal payment or undue advantage of any nature, to or by any person, with the intention of influencing the actions of any person or causing any person to refrain from any action. This topic is further covered in the CEI Africa Anti-Bribery and Corruption Policy.
Crowdlender	Crowdlending or crowdfunding platforms or hybrid forms domiciled in an EU member state, EFTA member state or UK , incorporated and licensed in accordance with national laws, regulations or decrees.
CTF	Counter-Terrorist Financing
Customer	This definition refers to either a Contributor, an Investee, a Grantee, a Guarantee, or a Crowdlender, with any reasonable interpretations necessary due to specific context as a Contributor, an Investee, a Grantee, a Guarantee or a Crowdlender being applicable in relationship to CEI Africa.
Designated Categories of Offences	(in line with FATF Recommendations and the respective interpretative note), participation in an organised criminal group and racketeering; terrorism, including financing of terrorism; trafficking in human beings and migrant smuggling; sexual exploitation, including sexual exploitation of children; illicit trafficking in narcotic drugs and psychotropic substances; illicit arms trafficking; illicit trafficking in stolen and other goods; corruption and bribery; fraud; counterfeiting currency; counterfeiting and piracy of products; environmental crime; murder, grievous bodily injury; kidnapping, illegal restraint and hostage-taking; robbery or theft; smuggling (including in relation to customs and excise duties and taxes); tax crimes (related to direct taxes and indirect taxes); extortion; forgery; piracy; insider trading and market manipulation.
EFTA	European Free Trade Association, an intergovernmental organisation of Iceland, Liechtenstein, Norway and Switzerland.
EU	European Union, an economic and political organisation between 27 European countries
EU law	Legislation approved by the European Parliament and the Council of the European Union.
FATF	Financial Action Task Force, the inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and the financing of terrorism.
Financial crime	Any kind of criminal conduct in the financial services or markets that include offences such as fraud or dishonesty, handling the proceed of crime, the financing of terrorism, market abuse, etc. In this definition, offence is to be intended as an act but also as an omission.

Foundation Manager	The entity selected to assist in the management of CEI Africa and its assets and investments as well as the provision of technical assistance by CEI Africa and the provision of grant activities of CEI Africa in accordance with the Foundation Management Agreement.
Fraudulent practice	Any action or omission, including misrepresentation that knowingly or recklessly misleads, or attempts to mislead, a person to obtain a financial benefit or to avoid an obligation.
Grantee	Developers of mini-grids who have been selected by CEI Africa in accordance with the RBF handbook and Policy for a result based grant of CEI Africa and who enter into a grant agreement with CEI Africa.
Guarantee	Natural or legal person or entity benefitting from the promise by the Guarantor to fulfil contract obligations towards CEI Africa if another party fails to pay or perform.
KYC	Know Your Customer
Investee	Any party which CEI Africa lends money to (debt) or invests in (equity).
Obstructive practice	Deliberately destroying, falsifying, altering or concealing evidence material to the investigation or the making of false statements to investigators, in order to materially impede an official investigation into allegations of a Corruptive practice, Fraudulent practice, Coercive practice or Collusive practice; or threatening, harassing or intimidating any person to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or any act intended to materially impede the exercise of an authorized party's access to contractually required information in connection with an official investigation into allegations of the above-listed practices.
ODD	On-going Due Diligence
PEP	Politically exposed person
Person	Any natural person, legal entity, partnership or unincorporated association
Risk-based Approach	An approach that involves tailoring the organisation's response and actions to fit the assessed risks. This approach allows to allocate resources to effectively mitigate identified risks and develop appropriate strategies whilst remaining aligned to CEI Africa priorities.
Sanctionable practice	Any Coercive Practice, Collusive Practice, Corrupt Practice, Fraudulent Practice or Obstructive Practice (as such terms are defined herein), which (i) is unlawful under EU, Dutch or other applicable law, and (ii) which has, or potentially could have, a material legal or reputational effect on CEI Africa or its Contributors.
Service provider	A third party, such as an entity or an individual that provides services to CEI with the provision of the service(s) being governed by a service agreement between them.
Source of Wealth	Customer's overall wealth generating activities. This includes family wealth (such as inheritance, gift, divorce or lawsuit settlements, etc.), income and revenue from business activities, or investment activities.
Staff	All those individuals employed by the Foundation Manager, with some form of employment agreement, who provide professional services to CEI Africa.
Supervisory Council	Supervisory entity of the conduct of management and on the general course of affairs of the Foundation.

UBO	Ultimate Beneficial Owner. The pseudo-UBO refers to natural person(s) who belong(s) to the senior management of a company, other legal entities, partnerships or other legal arrangements.
UK	United Kingdom

4. Roles and Responsibilities

The **Board of CEI Africa** has the ultimate responsibility for all aspects of the administration and management of the activities of CEI Africa. With respect to the compliance framework, the Board exercises its oversight in the following manner:

- Determining the Compliance Policy and presenting it to the Supervisory Council of CEI Africa for approval;
- Annually reviewing this Policy, determining any necessary changes and presenting them to the Supervisory Council for approval;
- Receiving and discussing the periodic and ad hoc Compliance reports prepared by the Compliance Officer of CEI Africa and by ASP on specific Compliance related measures;
- If applicable, receiving and reviewing any auditor's report on the appropriateness of CEI Africa´s compliance framework and, where necessary, supervising the implementation of the audit findings and recommendations.

The Board of CEI Africa will implement this Policy to ensure that CEI Africa complies and remains compliant with all the applicable requirements. Compliance with this Policy will be subject to regular controls and verifications, at a frequency determined according to the level of financial crime risks Africa is exposed to. The effectiveness of this Policy will be monitored and reviewed by the Board of CEI Africa periodically, but at least annually, taking into consideration its applicability and adequacy in the context of regulatory changes and operational capabilities and requirements of CEI Africa.

In the event the Compliance Officer is not able to perform their function, any Board member could act as, or temporarily replace, the appointed Compliance Officer in order to ensure that CEI Africa complies with all applicable requirements at all the times.

The **Foundation Manager of CEI Africa** is responsible for the execution of those tasks and activities needed to implement this Policy in relation to Grantees, Investees and Guarantees, such as:

- Responsible for CDD on prospective Investees, Grantees or Guarantees;
- KYC and AML/CFT compliance checks during monitoring of Investees' loan/equity compliance, monitoring of the compliance regarding grant agreements between CEI Africa and a Grantee;
- Monitoring of the compliance regarding guarantee agreements between CEI Africa and Guarantees.

The **advisor and** consultant **of the Foundation Manager for CEI Africa**, being Persistent Energy Capital LLC and GreenMax Capital Partners are responsible for:

- Data-collection of CDD/KYC data from Investees, Guarantees and Grantees.
- First assessment/opinion depending on the type of investment.

The Foundation Manager and the ASP will cooperate in good faith and support any other parties in the implementation of its responsibilities in this Policy.

Pursuant to the Service Agreement, the **ASP** is responsible for:

- The execution of the CDD and ODD processes as described in this Policy for Contributors and Service Providers of the Foundation
- Assessing financial crime related risks and completing CDD on Contributors and Service Providers
- Completing KYC on-going monitoring on Contributors and third parties;
- Liaising with the Foundation Manager on transactions of funds;
- On-going monitoring on Contributors and third parties
- Reporting unusual transactions;
- Providing periodic reporting to the Board of CEI Africa on the status of compliance with the provision of this Policy. See Annex 3 to this Policy for the Compliance Report Form
- Complying with record keeping requirements.

The **Compliance Officer** is responsible and accountable, under the delegation from the Board, for all the compliance matters defined in this Policy and in the following policies of the Foundation:

- Result-Based-Financing (RBF) Policy[1]
- Tax Compliance Policy[2],
- Anti-Fraud-, Anti-Bribery- and Anti-Corruption Policy,
- Gift- and Hospitality-Policy.

In particular, the Compliance Officer is responsible for:

- The effective implementation of this Policy and the other a.m. policies and for oversight on the CDD and ODD processes;
- Monitoring that the ASP fulfils all of its obligations to CEI Africa in relation to this Policy;
- Making recommendations to the Board in relation to CDD practices or to the provisions of this Policy;
- Providing a written report to the Board of CEI Africa and, if requested, to the Supervisory Council of CEI Africa, on an annual basis or on an ad hoc basis (see Annex 2);
- Remaining abreast of compliance requirements that are relevant to CEI Africa activities and providing regular updates
- Monitoring the appropriateness of the training and awareness programme of the ASP;
- Providing compliance related training to CEI Africa related parties, when necessary or requested.

The Compliance report will include an analysis provided by the ASP and a confirmation about the

- Implementation of the compliance procedures applied by the ASP;
- Level of professional knowledge and capacities of the responsible team of the ASP;
- Respective training in place at the level of the ASP.

[1]This policy is currently under development. The RBF policy is expected to be out of scope of the responsibility and accountability of the Compliance Officer. This will be confirmed once the RBF policy is finalized. Upon such a confirmation this policy will be removed from the list of policies the Compliance Officer is held accountable / responsible for.

[2]The Tax Policy will be developed with the input from a tax expert, under the responsibility of the Board of CEI Africa. Once ready, implementation of this policy - gathering and monitoring the data for tax compliance by the investees – will be performed by the Fund Services team of the Foundation Manager.

The Compliance Officer has sufficient professional experience and knowledge of the financial crime prevention regulatory framework to fulfil this role, and devotes sufficient time to the effective and autonomous exercise of these tasks. In addition, the Compliance Officer is granted the necessary authority for the discharge of the function, including the right to access CDD related documents. The independence, objectivity and decision-making autonomy of the Compliance Officer will not be impeded by the performance of any other function with respect to CEI Africa, and the workload will be adapted so that the work as Compliance Officer is not compromised.

The Compliance Officer has the right to start or recommend an investigation in relation to compliance matters, and will be able to perform on-site visits, at reasonable times and upon reasonable notice, of any of the CEI Africa's Customers and Service Providers (including the ASP) and/or oversight reviews, if deemed necessary, in order to ensure the ongoing effective monitoring of the delegated compliance functions.

5. CEI Africa Risk Appetite Statement

CEI Africa acknowledges that financial crime has an adverse impact on individuals, markets, and on community in general. For this reason, it takes responsibility for contributing to the protection of its Customers, and all stakeholders in general from any forms of financial crime or illegal behaviours. CEI Africa has **zero-tolerance** of breaches in relation to financial crime prevention requirements - and **zero-appetite** in conducting affairs that it believes are somehow engaged in criminal or unethical activities. CEI Africa is aware of the fact that it operates in developing – mostly identified as high risk – countries and understands the importance of determining its integrity risk appetite. Nevertheless, CEI Africa acknowledges the high risks that are inherently related to its business model, and accepts that in order to fulfil its mission and vision it adheres to an overall high integrity risk appetite. CEI Africa's manager and all the parties involved in the business model are trained and sufficiently knowledgeable to identify integrity risks and to comply with CEI Africa's integrity risk appetite.

The Board of CEI Africa has determined the following integrity risk appetite principles related to money laundering risks, terrorist financing risks and the circumvention of sanction risks.

Regarding Customers

- CEI Africa does not accept a Customer for which bribery or corruption is normal habit and part of the internal culture;
- CEI Africa does not accept a Customer of which the origin of funds is unclear or not plausible;
- CEI Africa does not accept the risk that a true positive hit on a sanction list is not followed-up adequately;
- CEI Africa does not accept a Customer (or related parties) that is mentioned on a Dutch, German, EU or UN sanction list or if such acceptance is prohibited under US Sanctions;
- CEI Africa accepts the risk that a Customer commits fraud and that it is discovered by CEI Africa too late (with financial and reputational damage as result);
- CEI Africa accepts the risk that the Ultimate Beneficial Owners (**UBO**s) of Customers are persecuted for criminal activities, but only if controlled and closely monitored until the judgement is final.

Regarding products, services, transactions and delivery channels:

- CEI Africa does not accept any activities or products that are illegal, or that are subject to sanctions (i.e., trade embargos);
- CEI Africa does not accept making (incidental) transactions with a bank account that has not been verified beforehand.

Regarding countries:

- CEI Africa does not accept a Customer that has its seat or is active in countries sanctioned by Dutch, German, European Union (EU) or United Nations Security Council (UN) sanctions, if such acceptance is in violation of Dutch law, EU or UN regulations;
- CEI Africa does not accept a Customer that has its seat or is active in countries sanctioned by United States (US) Department of the Treasury's Office of Foreign Asset Control (OFAC) Sanctions, if such acceptance is in violation of US law (safe for any exemption which may have been obtained beforehand);
- CEI Africa accepts a Customer that has its seat or is active in countries that are identified as high risk by European or Dutch law (if the risk is mitigated and monitored).

CEI Africa takes proportionate measures to identify and assess its money laundering, terrorist financing and financial crime risks. Risk factors related to Customers, products, services, transactions, delivery channels and geographical areas as described above are taken into account. The risk of non-compliance is also considered, and this is why the risk assessment and mitigation processes are ongoing – to ensure consistency and to address any specific circumstances.

5.1. General CDD Principles

- CEI Africa will apply CDD measures to existing and prospective Customers at appropriate times on a risk sensitive basis, or when circumstances change;
- Existing customers on framework agreements or repeat agreements will not be the subject of repeat CDD except in extreme circumstances, in the reasonable opinion of the Foundation.
- Typically CEI Africa would not accept a Customer if the CDD process could not be completed to an acceptable standard, and in observance of all applicable requirements;
- CEI Africa ensures that all parties involved in the CDD process receive the required training and awareness to enable them to conduct CDD in a good and complete manner;
- CEI Africa ensures sufficient capacity for the correct and complete execution of CDD as described in this Policy;
- Record of the CDD process and decisions are kept for each Customers, for at least five years following the termination of the commercial relation.

5.2. Purpose of CDD

The purpose of conducting CDD is to enable CEI Africa to:

- Identify the Customer and verify the Customer’s identity
- Identify the Customer’s UBO or Pseudo-UBO, and take reasonable steps to verify the UBO’s identity;
- Determine the purpose and intended nature of the commercial relation;
- Carry out ongoing monitoring on the Customer;

- Determine whether the natural person representing the Customer is authorized to do so and, where appropriate, identify the natural person and verify their identity;
- Take reasonable measures to verify whether the Customer is acting for itself or for a third party;
- Gain insight into the Customer's ownership and control structure.

The result of successful CDD means that CEI Africa knows, beyond reasonable doubts, with whom it is initiating or maintaining a commercial relation, with all the relevant risks being identified and managed.

If the CDD process indicates that a prospective Customer would pose an unacceptable risk for CEI Africa, then this Customer would be rejected.

5.3. Risk-based approach

CEI Africa does not offer any products or services nor engages in transactions which inherently pose potential direct risks of money laundering (ML), terrorist financing (TF) or of other Sanctionable Practices (i.e., cash-intensive products such as payment services or current accounts). Nevertheless, in recognition of potentially elevated risks of ML, of TF or potential risks of other Sanctionable Practices posed by the country risk profile of CEI Africa's target countries (Official Development Assistance/ODA-recipient countries in Sub-Sahara Africa), as well as the inherently long-term nature of the majority of its financing and grant making, CEI Africa places great emphasis on integrity and good governance principles and is committed to the highest standards of the prevention of ML, in full alignment with the applicable requirements in the Netherlands and in the EU (or other countries with extra-territorial effect).

The Foundation Manager and the ASP will adopt a risk-based approach when assessing prospective Customers or conducting on-going monitoring on existing ones. This approach ensures a more appropriate allocation of resources and yields a better result by channeling more attention to high-risk Customers and determining the level of CDD that is required. An initial risk assessment is performed for the identification of a risk level (i.e., low, medium high). The risk classification determines the extent of CDD to be performed and also the frequency for periodic reviews. The risk classification also determines the extent of applicable CDD level: *simplified* for a low-risk classification, *standard* for a normal risk classification, or *enhanced* for a high-risk classification. Accordingly, the risk classification defines the standard frequency of monitoring over Customers:

- Customers with a **low-risk** classification are re-assessed **every three (3) years;**
- Customers with a **normal risk** classification are re-assessed **every two (2) years;**
- Customers with a **high-risk** classification are re-assessed **every year.**

The risks that are considered in this assessment include:

- Customer risks (i.e., identification of UBO, presence of PEPs, organisational structure and governance; transparency and cooperation to the CDD process)
- Transaction risks
- Country risk (i.e., the jurisdiction in which the Customer operates or resides, etc.)

Other types of risks, such as credit risks, are not in scope of this Policy.

6. Overview of the CDD Process

The typical CDD process (standard CDD) includes the following stages:

- Preliminary risks assessment to assign an initial risk score based on
  - Customer risk
  - Business Activity/ Product/Sector Risk
  - Domiciled Country risk
- Identification and Verification of the Customer and expected involved parties
  - Collection and review of relevant documents (i.e., identity documents, corporate documents, policies, reports, etc.)
  - Identification and verification of directors and other representatives of the Customer, including those individuals who are authorised to represent the Customer
  - Assessment of the ownership and governance structure
  - (Where possible) on-side verification and desk due diligence
- PEPs, sanctions and adverse media screening on the Customer, the UBO(s), directors, representatives and all involved parties (i.e., shareholders, etc.)
  - World-check tools and automated daily screening
  - Interned searches
- Determination of the source of funding of the Customer's business
- Final assessment and risk assessment
  - Preparation of a CDD Memo to address all the relevant points, including an overview of the prospective Customers and of the documents received
  - Final risk score with the agreement of the measures and monitoring items to put in place
  - Plan for the ongoing monitoring

A typical CDD file would include the following documents and data collected from the Customer:

- The identification and verification of the identity of the (prospective) Customer and related persons (e.g., UBOs, pseudo UBOs, Board Members (or equivalent) and representatives);
- Purpose and intended nature of the commercial relation between CEI Africa and the Customer;
- The source of funds used in the Customer's business;
- The Customer's ownership and control structure;
- Proof of conducted sanction lists/ PEP/ bad press screening;
- Company documents, including audited financials and evidence of a bank account's ownership;
- Risk assessment per type of risks and the risk classification;
- CDD related minutes of meetings or calls with the Customer;
- The Customer's transaction profile (if applicable);
- Any other documents and data that is considered relevant or necessary for that Customer.

6.1. Extent of the CDD Process

Depending on the overall risk category of the Customer, which reflect the type of risk posed to CEI Africa, the following types of CDD could apply:

Customer risk classification (whether prospective or existing)	Description of the process
Low risk	Simplified CDD can be applied
Normal risk	Standard CDD is appropriate
High risk	Enhanced CDD is required
Unacceptable risk	No commercial relation can be established – or an existing one is terminated

6.1.1. Simplified CDD for low-risk Customers

CEI Africa might decide to conduct simplified CDD in case it establishes that the commercial relation with a Customer entails a low risk of money laundering or terrorist financing. CDD is not omitted but its intensity is aligned with the risk associated with the type of Customer, transaction or jurisdiction (i.e., it could be the case for a EU based donor). The conclusion that simplified CDD is appropriate is always based on a risk assessment and without assuming by default a lower risk category. This is done with an initial risk analysis, taking into account the risk factors on which bases the *potentially* lower-risk category is identified. In case simplified CDD is considered appropriate, then:

- Sufficient data is collected to demonstrate that the application of simplified CDD was appropriate;
- The collected data and the determination based thereon are kept up to date;
- The commercial relation is subject to ongoing monitor.

Factor that could determine the application of simplified CDD typically are:

- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- Regulated entities in an EEA member state;
- Public administrations or enterprises;
- Customers that are resident in geographical areas of lower risk, such as third countries effective systems to combat money laundering and terrorist financing, or with effective implementation of FATF recommendations

Simplified CDD results in the request and collection of less information and proofs from the Customers, most of which is publicly available (i.e., registration with local authorities, government-issued documents, etc.).

Simplified CDD measures are no longer acceptable whenever there is a suspicion of money laundering or terrorist financing, or when specific higher risk scenarios apply.

6.1.2. Enhanced CDD for high-risk Customers

If during the standard CDD process it appears evident that the Customer (whether prospective or existing) is classified as high-risk, then the CDD process is extended to become enhanced CDD. This means asking more information and proof on the particular aspect(s) that results in the high risk, and/or that are not clear (enough), according to a Risk-based Approach. It could be the case if the Customer:

- Poses a higher risk of money laundering or terrorist financing; or

- Is domiciled or established in a jurisdiction with strategic deficiencies so to pose significant threats to the EEA financial system (e.g., high risk country).

Enhanced CDD is conducted on a risk-based approach, meaning that it is assesses what additional information and proof is necessary in order to be able to adequately analyse and mitigate the integrity risks related to a (prospective or existing) Customer. A high-risk Customer is asked to provide **extra information** in relation to the business, which is also validated from an independent and reliable source. It is also subject to **more frequent and in-depth monitoring**. In addition, approval from the Board of CEI Africa is needed to initiate a commercial relation with a high-risk Customer.

Examples of these extra measures to be taken applying a Risk-based Approach might include requesting a copy of notarized passport, or validation of the assets used in relation to the Customer activities (e.g., audited sales and income tax return), conducting more extended research for adverse media news, etc, or increasing the frequency and the scope of the monitoring. For high-risk cases, the Board approval is a required condition for proceeding with the provision of services from CEI Africa.

6.1.3. UBOs

An UBO is defined as a natural person who is the ultimate owner of, or controls, a Customer, or the natural person on whose behalf a transaction or activity is executed. This is done through holding, directly or indirectly, more than 25% of the shares, voting rights or ownership interest in the company, including the holding of bearer shares, or through other means, including conditions for consolidation of annual accounts.

If, after exhausting all possible means and on the condition that there are no grounds for suspicion, no natural person qualifies as UBO, or if there are any doubts as to whether a natural person is the UBO or has control or is the natural person on whose behalf a transaction is made, the natural person(s) who belong(s) to the senior management of the company, other legal entity, partnership or other legal arrangements, qualifies or qualify as so-called **'pseudo-UBO'**.

If, during the CDD process, it is not possible to establish the identity of the UBO (or the pseudo-UBO), a commercial relation will not be initiated.

6.1.4. PEPs

International standards issued by FATF recognise that a PEP may be in a position to abuse their public office/function for private gain and/or may use the financial system to launder the proceeds of this abuse of office. Also, PEPs can be vulnerable for corruption (e.g., the receipt of slush money[3]) and fraudulent practices (e.g., embezzlement of public money). CEI Africa takes appropriate measures to determine how much influence a PEP has in the transactions (to be) made by or on behalf of the Customer. PEP status itself does not, of course, incriminate individuals or entities. As FATF states,[4] '*these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatising PEPs as such being involved in criminal activity*'. This is to avoid that a PEP is unduly denied access to financial services. It does, however, put the Customer, or their UBO, into a higher risk category.

[3] Money put aside to be used to bribe or influence, especially in a political context.

[4] Recommendations 12 and 22

A PEP is a natural person who is or who has been (in the past 12 months) entrusted with prominent public functions, including any of the following:

- Heads of State, heads of government, ministers and deputy or assistant ministers;
- Members of parliament or of similar legislative bodies;
- Members of the governing bodies of political parties;
- Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory bodies of State-owned enterprises;
- Directors, deputy directors and members of the board or equivalent function of an international organisation.

None of these public functions shall be understood as covering middle-ranking or more junior officials (secondary or lower level). In addition, the PEP status also applies to a PEP's:

- Direct family members, being:
  - ✓ spouse (or a person considered to be equivalent to a spouse);
  - ✓ children and their spouses (or persons considered to be equivalent to a spouse);
  - ✓ parents;
- Close-associates, being:
  - ✓ natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close BRs, with a PEP; or
  - ✓ natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP.

Typically PEPs are identified during the screening process.

Natural persons not qualifying officially as PEP anymore because they are no longer entrusted with a prominent public function:

- Are still screened via Internet searches for bad press, e.g., fraud, corruption, bribery; and
- Remain subject to enhanced CDD for as long as necessary, but at least for 12 months, until this person no longer brings the higher risk associated with political prominent persons.

In case the UBO of a Customer is also a PEP, then enhanced due diligence will apply and approval is needed by the Board of CEI Africa, following the recommendation of the Compliance Officer.

7. Financial Sanctions

Acting in violation of sanctions is an **economic offence** and, therefore, a criminal offence. Financial sanctions are restrictions put in place by the government or the multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds, and economic resources in order to achieve a specific foreign policy or national security objective. The United Nations Security Council, the EU, the Netherlands, the Federal Republic of Germany, the World Bank

are all able to designate targets by way of financial sanction legislation. Where a financial sanction takes the form of an asset freeze, it is generally prohibited to:

- Deal with the funds or economic resources belonging to, owned, held, or controlled by a target;
- Make funds or economic resources available, directly or indirectly, to or for the benefit of a target;
- Engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions.

Certain financial sanctions may prohibit the provision of financial services, directly or indirectly, to a target or for the significant benefit of a target. Financial sanctions can apply to individuals, entities, sectors, and governments, and can also apply to all the residents of a particular country**. It is a criminal offence to make funds, economic resources or, in certain circumstances, financial services available to those persons or entities listed as the targets of financial sanctions**. During the screening process, and then on an on-going basis, CEI Africa or any other delegated parties, will check that Customers, and any affiliated parties, Service Providers and any parties with which it engages a business or commercial activities appear on a sanction list (I.e., individuals, entities, sectors). In case of a true positive match, the Compliance Officer is immediately notified so that the best course of action can be decided with the Board of CEI Africa.

CEI Africa is aware that failure to consciously report an unusual transaction is an economic offence within the meaning of Article 1(2) of the Economic Offences Act (WED).

8. On-going Due Diligence

On-going due diligence (ODD) is routinely conducted to ensure Customer's data and documents are kept up to date so that the commercial relation does not pose adverse risks for CEI Africa.

As mentioned before, all Customers and related parties are subject to on-going automated screening against PEPs and financial sanction lists through World-Check/Finscan on a daily basis.

Depending on the extent of CDD applied, on-going due diligence (**ODD**) is performed on a risk-sensitive basis, with exhaustive monitoring measures to appropriately addressing money laundering and terrorist financing risks, as well as other financial crime risks (i.e., bribery and corruption, non-compliance with financial sanctions. These measures are designed to make the perpetration of any forms of financial crime more difficult and are put in place for the entire duration of the commercial relation between CEI Africa and its Customers.

ODD can be conducted on a periodic basis, with the frequency dictated by and associated to the Customer's risk category:

Customer risk classification	Frequency of the monitoring
Low risk	Every 3 years
Normal risk	Every 2 years
High risk	Every year (or more often if required so)

Event-driven review can be generated by suspicions that a Customer is being associated to money laundering, terrorist financing or any other forms of financial crime. Likely indicators could be:

- Ambiguity in relation to the Customer underlying parties or beneficiaries;
- The Customer is unwilling to provide up to date documents;
- Customer's refusal to cooperate with ad hoc reviews;
- Any aspects of the commercial relation that deviate from the Customer's profile.

PEPs are subject to on-going monitoring and remain subject to monitoring for as long as necessary, but at least for 12 months following the termination of their public function, until they no longer pose CEI Africa the typical risk associated with PEPs.

A Customer ODD review consists of a reassessment of a CDD file after a certain set term. An "ODD self-certification" letter is sent to the Customer who are asked to confirm that:

- it has reassessed their documents and data are still up-to-date;
- if there have been materially relevant changes.

Depending on the Customer's response, CEI Africa might additionally review the Customer's risk profile, in its risk classification. All elements mentioned in the CDD Process are included in this reassessment, with existing information updated where necessary, or additional document obtained, if required.

Once the identity of a Customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification). As risk dictates, however, appropriate steps are taken to ensure that appropriate information on the Customer is kept up-to-date.

8.1. Forced Termination

Based on the results of ongoing monitoring or of a triggering event, the classification of an existing Customer may change to an unacceptable risk classification, in which case the commercial relation with that Customer needs to be ended as quickly as legally possible.

Legal agreements with the Customer (especially with equity type of Investee) will include a clear exit strategy, which would allow CEI Africa exit an investment as soon as reasonably possible, or take steps to resolve the triggering events. This is to make it clear the circumstances under which the commercial relation with the Customer will be terminated, or the process by which the trigger event will be resolved. Nevertheless, in light of the nature of the business that CEI Africa operates, a short-term exit is not always feasible to, nor the attempt to restructure the terms of the agreement. In such circumstances of unacceptable risk, CEI Africa carefully records evidence of how it pursues an exit in the shortest term possible, of all the efforts and progress made, and of any measures it has put in place to mitigate risks arising from the unacceptable risk situation.

9. Record Keeping and Data Protection

Record keeping is an essential component of a financial crime prevention regime. CEI Africa safely maintains records of its activities, commercial relations and related transactions for audit-trail purposes, and reporting obligations (if necessary). CEI Africa digitally saves all documents and data collected during the CDD process. To comply with applicable requirements, CEI Africa keeps:

- Customer or its UBO/Pseudo UBO information (such as a copy of their identification documents and other obtained evidence);

- Transactions records (such as payment to individuals and bank account details);
- Details of the internal suspicions reported to the Compliance Officer
- Details of on-going monitoring and compliance monitoring.

CDD related information is kept and made accessible for five years from the date of the termination of the commercial relation, or for five years after the execution of the transaction in question. CEI Africa ensures that any records, held in whatever medium and language, can be accessed in an accurate and timely manner so to respond promptly and fully to questions from external reviews or audit.

Personal data collected during the CDD process is only processed by CEI Africa for the purpose of preventing money laundering and terrorist financing, and is not further processed for commercial or other purposes that are incompatible with that purpose. Before entering into a commercial relation, CEI Africa informs the Customer of the applicable obligations for the processing on personal data. Prospective and existing Customers are informed that CEI Africa might use their personal data for the purpose of detection and prevention of fraud, money laundering and terrorist financing, and any other forms of financial crime. After the expiry of the legally required retention period, personal data obtained for the purpose of completing CDD is destroyed.

Further details can be found in the CEI Africa Privacy Statement.

10. Review of this Policy

This Policy will be reviewed by the Compliance Officer periodically, and at least annually. Recommendations for amendments, if needed, will be made to the Board of CEI Africa, which will report to the Supervisory Council of CEI Africa at least annually on the implementation of this Policy, on the compliance risks of CEI Africa as well as on legal and regulatory changes in the context of this policy applicable to CEI Africa.

Training will be provided to ensure all the parties involved in the CDD and ODD processes are familiar with the requirements and the best practice, so to achieve high quality standards and compliance with the provisions of this Policy.

Annexes
Annex 1: Due Diligence on Service Providers
Annex 2: Compliance reporting topics (compliance officer)
Annex 3: Compliance reporting form (ASP)

Annex 1 – Due Diligence on Services Providers

A Service Providers is defined as a third party, such as an entity or an individual that provides services to CEI Africa or its Foundation Manager, with the provision of the service(s) being governed by a service agreement between them.

Once a Service Provider has been selected, due diligence is conducted to ensure CEI Africa has addressed the potential risks (i.e., involvement in any forms of financial crime and reputational risks) that a commercial relation with the selected Service Provider can pose. The following risk factors are typically considered when assessing the risk exposure:

- Jurisdiction of the Service Provider (i.e., whether the Service Provider is located and operates in a low, medium or high-risk country). All EU and ETFA member states, as well as the UK, the United States and Canada are considered low risk
- The amount of the contract
- The expected length of the partnership between CEI Africa and the Service Provider
- The reputation and integrity of the Service Provider
- The impact on CEI Africa operations in case of poor performance, disruption of the service, etc. from the Service Provider

The combination of these factors determines the risk classification associated to the Service Provider and the level of due diligence to perform:

- **Simplified** due diligence for low-risk classification
- **Standard** due diligence for medium risk classification
- **Enhanced** due diligence for high-risk classification

Applying due diligence on the selected Service Provider aims to establish the following aspects:

- Validation of necessary licenses and registrations
- Identification of the representative(s) of the Service Provider (I.e., those CEI Africa will be in contact with)
- Screening of the entity and its related parties (I.e., financial sanctions and adverse media)
- Collection and verification of relevant corporate documents (I.e., for standard and enhanced due diligence)
- Verification of the Service Provider's bank account (I.e., for standard and enhanced due diligence)

The level of due diligence applied is then reflected in the level of on-going due diligence and monitoring to be conducted, in terms of frequency and intensity.

The table below details the different types and route of Procurement and the recommended type of CDD to be applied before a commercial relation is established with the selected Service Provider(s).

Simplified due diligence can be conducted in the following circumstances:

- The Service Provider is located/operates in a low-risk jurisdiction
- The amount of the contract is below €10,000
- The term of the contract is less than 3 months
- The service to be provided would not materially affect CEI Africa's operations in case of disruption of the service

It consists in the collection of all information and documents to cover the points listed above. In many cases, information can be publicly available and accessible from public sources.

Standard due diligence can be conducted in the following circumstances:

- The amount of the contract is between €10,000 and €99,999
- The term of the contract is between 3 and 12 months
- The disruption of the service provided would require some attention but would not stop CEI Africa's operations

The due diligence process would be similar to the simplified one, although the required information and documentation would not be publicly available, hence it needs to be obtained by the Service Provider. In addition, more than one Service Providers should be considered for selection, and a short Memo filled to describe the selection and the vetting process.

Enhanced due diligence should be conducted in all other cases, such as

- The Service Provider is located/operates in a high-risk country
- The amount of the contract is above €100,000
- The term of the contract is over 12 months
- The disruption of the service provided could require a stop CEI Africa's operations (if applicable)

Depending on circumstances, a copy of the passport of the person(s) representing the Service Provider should be required, as well as a letter signed by the bank to confirm the ownership of the bank account. The Memo needs to be approved by the Compliance Officer and the Board of CEI Africa. On an annual basis, the file including the Service Provide information and documentation is reviewed to ensure it is still relevant and up to date.

Annex 2: Topics for the Compliance Report of CEI Compliance Officer

The CEI Africa Compliance Officer periodically reports to the Board and to the Supervisory Council in relation to the Compliance Policy (typically every 3 months or more often if needed). The Compliance report covers the following points:

- Status of compliance with the provision of the Compliance Policy
- Summary of the CDD and ODD processes (e.g., description of the Customers, high-risk classification, true positive hits during the screening process, unusual cases, termination of commercial relations, etc.)
- Considerations on the Compliance report received by other parties (i.e., ASP)
- Recommendations in relation to the implementation of the Compliance Policy
- Training related matters, including considerations over the level of professional knowledge and capacities of the staff involved in implementing compliance related activities under the Compliance Policy

Annex 3: Compliance Reporting Form (Template) for IQEQ

STICHTING CEI Africa

To : The Board of CEI Africa and the Compliance Officer
From : IQEQ (Netherlands) B.V. (Administration Service Provider)
Date : [DATE]
Discussed and approved: [DATE]

This report summarises Compliance related actions taken in relation to prevention of money laundering, prevention of terrorist financing and other Sanctionable Practices by the Administration Services Provider (ASP) for the period [PERIOD] ("Period"), attached hereto

- Number of Customer on-boarded/rejected/pending approval
- Description of the Customers
- Number of high-risk Customer identified
- Number of unusual transactions (and if reported or not)
- Description of any deviations from the standard CDD process, as described in the CEI Africa Compliance Policy
- Summary of the on-going monitoring process
- Any relevant recommendations or concerns to report

Customer	Risk profile	Review frequency	Date last review	Next review