

JSC "Georgian Energy Development FUND"

Anti-Money Laundering and Anti-Terrorism Financing Policy

Article 1 - Introduction

1.1. Joint-stock company "Georgian Energy Development FUND" (hereinafter "FUND") is a joint-stock company managed and 100% owned by the Ministry of Economy and Sustainable Development of Georgia.

1.2. The mission of the FUND is to promote the realization of the energy potential of the country and to find appropriate FUNDS by developing projects and their effective implementation. The main goals of the FUND are to find promising projects of renewable energy sources and to promote their development (hereinafter "projects"). Based on this, the FUND mainly carries out the following activities:

1.2.1. conducting preliminary research works;

1.2.2. preliminary technical and economic evaluation of projects;

1.2.3. preliminary environmental impact assessment;

1.2.4. finding investors and increasing their interest in existing projects.

1.3. To achieve these goals, the FUND cooperates with investors and third parties, and provides them with certain services, including:

1.3.1 preparation of all documents necessary for construction, including obtaining construction rights and licenses;

1.3.2 finding a design firm and purchasing a complete construction project;

1.3.3 preliminary schematic processing of the project or preparation of the preliminary feasibility report;

1.3.4 Monitoring of the construction process.

1.4. The FUND acts in accordance with the highest ethical and professional standards and expresses its commitment to follow the highest standards of combating money laundering (hereinafter "AML") and the financing of terrorism (hereinafter "CFT") in its activities and is committed to acting in accordance

with internationally recognized principles and norms of AML/CFT and the applicable legislation of Georgia.

Article 2 - Objectives

2.1. The present "Anti-Money Laundering and Anti-Terrorism Financing Policy " (hereinafter - the "Policy") defines the basic principles and measures of the FUND in AML/CFT, which it uses both in its own activities indicated above, and in relations with investors, partners and contractors/suppliers in order to implement projects (hereinafter collectively referred to as the "Contractors") by the FUND.

2.2. The main purpose of this policy is to define a number of measures and ensure their continuous implementation, which will effectively prevent the FUND and its staff from:

2.2.1 involvement in money-laundering and/or being used for money-laundering while receiving FUNDS from investors or providing services to contractors for the purpose of project implementation; and/or

2.2.2. involvement in the financing of terrorism and/or have been used to finance terrorism while making financing/payments to contractors for project implementation.

2.3 The FUND will cooperate only with those counterparties who carry out legal business and have received monetary FUNDS from legal sources.

Article 3 - Applicability

3.1. The principles and procedures described here are used in all activities of the FUND, which are related to the implementation of projects. All employees of the FUND are obliged to follow this policy. Any employee who violates the rules set forth in this policy or allows others to violate them will be subject to appropriate disciplinary action (as provided in the internal regulation of the FUND) and may be subject to civil or criminal liability (in accordance with applicable law).

Article 4 – General Definitions

4.1. Money laundering:

4.1.1. conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illegal origin of the property or assisting any person

participating in the implementation of such activity to avoid the legal consequences of such person's actions;

4.1.2. Concealing the true nature, source, location, disposition, movement, or rights in possession of property, knowing that such property was obtained as a result of criminal activity;

4.1.3. Acquiring, possessing, or using property with the knowledge that the property was obtained as a result of criminal activity.

4.2. Terrorism-financing

Collecting or providing financial FUNDS in any way, directly or indirectly, with the intention that they will be used, or with the knowledge that they may be used, in whole or partially to support a terrorist offense and to carry out terrorist activities, and/or provide services to a terrorist or a terrorist organization with prior knowledge, providing a hideout or shelter to a terrorist and/or providing resources or other material support to a terrorist or a terrorist organization.

It is not obligatory that the FUNDS be actually used in whole or partially to commit or support any of the above crimes. It is not required that the offender knows for which specific crime the FUNDS are intended .

4.3. Ultimate Beneficial Owner (hereinafter "UBO"):

A person who directly or indirectly owns 25% or more of the shares or voting shares of a legal entity or otherwise exercises full control of the legal entity.

4.4. Politically Exposed Person (hereinafter "PEP"):

A person entrusted with the performance of important public functions. In particular:

- a) heads of state, heads of government, ministers and deputy ministers or assistants;
- b) Members of Parliament and similar legislative bodies;
- c) members of governing bodies of political parties;
- d) members of Supreme Courts, Constitutional Courts or other high-level judicial bodies whose decisions are not subject to further appeal, except for specific cases;
- e) members of the board of the Chamber of Auditors or the Central Bank;
- f) members of administrative, management or supervisory bodies of state enterprises;

g) directors, deputy directors and members of the board of directors or bodies of equivalent functions of international organizations;

h) other persons who are considered as PEPs in accordance with the applicable laws.

Other terms used in this policy have the meanings defined by the Law of Georgia No. 5226-I "On the Promotion of Prevention of Money Laundering and Financing of Terrorism" dated as of October 30, 2019

Article 5 - AML Compliance Officer

5.1. In order to supervise violations of this policy, the FUND appoints a Compliance Officer (hereinafter "Compliance Officer").

a) The compliance officer ensures the overall supervision of the policy within the competence established by the policy , in particular, the compliance officer:

- determines policy compliance for FUND employees;
- resolves other issues arising in the process of proper implementation of this policy.

In addition and notwithstanding the above, since the initiation, development and implementation of projects in the FUND are ensured by the relevant structural units/employees of the FUND, from the date of approval of this policy, in the case of any project, the relevant employee/structural unit of the FUND implementing/supervising the project ("Project Manager") shall Submit the following information to the Compliance Officer:

- results of examination of counterparties;
- AML-Questionnaires completed and signed by the counterparty and other typical documentation required to implement this policy.

b) The compliance officer is an employee of the FUND, appointed by the director, on the recommendation of the audit committee. The compliance officer's authorization starts on the date of the director's order. The compliance Officer can be dismissed by the Director. The compliance officer is obliged to follow the decisions and orders of the director. The compliance officer's authority/responsibility is terminated based on the submission of a written statement by the compliance officer, on the date of the application and/or upon termination of the employment contract with the Compliance Officer.

The Compliance Officer is accountable to the Director. In case of termination of the authority of the compliance officer, the director is obliged to appoint another person within 10 working days after the occurrence of any of the mentioned circumstances.

c) In order to be able to ensure the proper implementation of this policy, the compliance officer must meet the official requirements, in particular, he/she must know the AML/CFT laws of Georgia, the best international practices and market standards in the field of AML/CFT, to have relevant certificates of qualification in AML/CFT and to understand the process of practical implementation of AML/CFT measures.

Article 6 - Expertise of counterparties

Expertise of counterparties (hereinafter "CDD") is carried out by the FUND employee/structural unit - project manager authorized to initiate/develop/implement the project. This process includes

6.1. Counterparty identification and verification

In order to identify and verify the counterparty, the Project Manager will obtain and submit in writing to the Compliance Officer the following information:

- ✓ Name and surname of the counterparty in full (in the case of a natural person);
- ✓ Name of the counterparty (in the case of a legal entity);

- ✓ Identification data of the representative of the counterparty:
- ✓ UBO (UBOs) of the counterparty.

The relevant project manager of the FUND is obliged to cooperate with the compliance officer and act in accordance with the instructions of the compliance officer.

6.2. Counterparty risk assessment

For the purpose of risk assessment/profiling of the counterparty, the project manager will obtain and submit in writing the following information to the compliance officer :

- purpose of employment and economic justification;
- country of residence/registration of the counterparty (in the case of a company, additionally the name and country of residence of its UBO (or UBOs); identity documents;
- any information about counterparty (its UBO/UBOs) participation in money laundering / financing of terrorism;
- in case of a legal entity, an extract from the relevant register/information about the good corporate standing of the counterparty;
- in case of a legal entity - organizational structure;
- documentation confirming representation.

6.3. The project manager is obliged to ensure that the relevant counterparty fills in and signs the standard AML-questionnaire of the FUND.

6.4. The compliance officer verifies the information obtained and submitted by the project manager.

6.4. The above list of information/documents is not complete so it may be updated/changed by the compliance officer, and in any case it should be noted that the main purpose of identification and verification of the counterparty is to determine the status of the enterprise and its UBO(s).6.5. The compliance officer may reasonably clarify/request any additional information from the contractor with the project manager in order to properly evaluate the above information/documents, assess and identify

the risks related to the potential contractor through the appropriate risk matrix (refer to Annex 1) and in accordance with the risk-based approach .

6.6. The FUND/project manager is obliged to ensure that copies of the above documents are kept for at least a 5-year period after the termination of business relations with the counterparty.

6.7. The FUND is obliged to refuse cooperation with counterparties who are distinguished with unacceptable high risk.

6.8. Cooperation permission for high-risk contractors, cooperation permission (in addition, the signing of the relevant contract/agreement is interpreted as permission) is given by the director of the FUND based on the written submission of the project manager. In case of medium and low risk counterparties, entering into an agreement with the counterparty does not require the permission of the director and/or compliance officer.

6.9. The project manager is obliged to submit a written notification to the compliance officer regarding any relevant changes in the information provided by the counterparties. The compliance officer ensures monitoring of changes in the risks following the examination of the contractors presented by the project manager and, if necessary, determines the need for re-assessment of the risks based on the information received from the counterparty. Such risks are assessed:

6.9.1. in case of a high-risk counterparty - annually;

6.9.2. in case of a medium risk counterparty - once in every 2 years;

6.9.3. in case of a low-risk counterparty - one in every 3 years.

6.10. All relevant employees of the FUND are required to disclose in writing any information related to counterparty risk assessment, counterparty examination and/or monitoring of post-examination risk changes to the Compliance Officer

6.11. In the event that the Project Manager/any FUND employee fails to provide the Compliance Officer with information related to the Counterparty in accordance with this Policy, the project manager/any employee of the FUND is responsible for strictly following this policy and obtaining/keeping relevant information.

Article 7 - Reporting

7.1. All employees are required to notify the Compliance Officer if they become aware of or suspect that money laundering or terrorist financing is taking place in the course of their activities, or if they obtain information that makes them aware of, or suspect, or doubt that a certain person is involved in money laundering and obtaining the receipt of criminal income, terrorist activity or financing of terrorism.

7.2. If any employee of the FUND has information about the activities of the FUND, its management or other employees, which violate the requirements of this policy or their activities can be considered as money laundering or financing of terrorism or is somehow related to money laundering or financing of terrorism, such employee shall submit to the Compliance Officer a report or, at own discretion, an anonymous report (for more details, see the FUND's Whistleblower Protection Policy) and all evidence.

7.3. Upon receipt of written notice pursuant to this Policy, the Compliance Officer is authorized to instruct any body, commission, committee, associate of the FUND, relevant services/departments of the FUND and their heads and/or any person deemed appropriate by the Compliance Officer, in order to study the received report and receive support in the development of relevant guidelines and recommendations.

7.4. Regarding the results of the investigation and the recommendations of the compliance officer, the appropriate decision is made and executed by the director.

Article 8 - Trainings

8.1. The Compliance Officer, directly or through third parties hired for this purpose, conducts training for all employees of the FUND involved in the implementation of projects to ensure that employees are familiar with this policy, their obligations, and that they understand the basic AML/CFT principles and objectives set forth herein. Such trainings should be held annually.

8.2. Notwithstanding the foregoing, each employee is required to independently familiarize and strictly adhere to the requirements of this policy.

Article 9 - Internal audit

9.1. The Audit Committee of the FUND conducts an internal audit of the implementation of AML/CFT measures, evaluates their effectiveness and sufficiency in preventing money laundering and terrorist financing practices in the FUND. The results of such audit shall be submitted to the Director by the Audit Committee. The FUND may also hire a third party to conduct the audit. Based on the results of the audit, this policy may be subject to updating.

9.2. Audit should be conducted at least once every 2 years.

Article 10 - Final Provisions

10.1. This policy is effective from the date of approval by the Director of the FUND in his respective order.

10.2. This policy is not retroactive.

ANNEX 1

Risk matrix

An incomplete list of indicators that need to be taken into account to assess and determine the level of risk of the counterparty.

Risk level	Risk indicator	Possible sources of risk type determination
Unacceptable high risk	Counterparties, their UBOs, representatives or employees are: <ul style="list-style-type: none"> ● Listed with persons linked to terrorism, or officially suspected of financing terrorism and/or money laundering ● Registered or residing in countries that facilitate international terrorist activities, or countries subject to sanctions, embargoes or similar measures have been taken by the United Nations Poverty Reduction Agency 	Publicly available list of terrorists (refer to https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list/ or information from other sources) Websites of foreign or local government bodies: United Nations website for information on sanctions imposed by the Security Council

	<p>or the Georgian legislation, and this is known from reliable sources</p> <ul style="list-style-type: none"> Owned or controlled by the Russian Federation Counterparties who provide insufficient, false or questionable information or avoid providing complete information, or (including their UBOs, if any) it is impossible to establish the purpose and economic justification of the cooperation, or it is impossible to carry out identification and verification 	<p>https://www.un.org/sc/suborg/en/sanctions/;</p> <p>US State Department website http://www.state.gov/j/ct/list/c14151.htm</p>
<p>High risk</p>	<ul style="list-style-type: none"> Counterparties; their UBOs, representatives or employees are based in or located in countries that are considered high-risk countries according to the FATF recommendation, or in the Russian Federation; Counterparties, their UBOs, representatives or employees are PEPs or their family members, or close associates of such PEPs; with reliable sources, the mass media negatively covers the activity of the counterparty, which indicates that it may be involved in money laundering or terrorism financing; non-profit, charitable, religious organizations (except international charitable and non-profit organizations); 	<p>Information from publicly available sources, for example: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate);</p> <p>Lists of PEPs</p> <p>Information from a potential counterparty questionnaire, documents submitted for AML identification, financial reports, media sources, websites of foreign and local agencies.</p>

	<ul style="list-style-type: none"> • Lottery organization and gambling companies (including casinos and electronic (visual) casinos); • companies providing currency exchange and/or money transfer services (except banks), virtual currency operators; • Companies whose activities are related to the production and sale of weapons, defense equipment (arms dealers / manufacturers) • Foreign financial institutions (except for those registered in EU or FATF member countries, with which correspondent relations are established) • Counterparties requesting cash settlements, payments from third parties that have no clear or logical connection with such counterparties or transaction operators 	
Average Risk	Counterparties that do not fall into the description of "low risk", "high risk", and "unacceptable high risk"	
Low Risk	<ul style="list-style-type: none"> • State bodies • State enterprises • Publicly traded companies • EU entity, person, body, office or agency • International organizations and institutions. • If there is no indication of high or unacceptable high risk. 	Information from a potential counterparty's questionnaire, documents submitted for AML identification, financial reports, media sources, websites of foreign and local agencies, stock exchanges, etc.