POLICY

of VEB.RF and VEB.RF’s Entities

on Combating Money Laundering and the Financing of Terrorism and Proliferation
1. General ........................................................................................................................................ 3
2. Basic Terms, Definitions and Abbreviations .............................................................................. 3
3. Goals and Principles of CML/FT&P ............................................................................................ 5
4. Uniform Bans and Restrictions ................................................................................................... 5
5. Basis of the CML/FT&P System .................................................................................................. 6
6. Particularities of CML/FT&P Internal Controls ......................................................................... 8
7. KYC Procedures .......................................................................................................................... 10
8. Risk Assessment ........................................................................................................................ 12
9. Monitoring of Transactions ......................................................................................................... 14
10. Staff Training ............................................................................................................................ 15
11. Storage and Confidentiality of Information .............................................................................. 16
12. Final Provisions ......................................................................................................................... 18
1. GENERAL

1.1. The Policy of VEB.RF and VEB.RF’s Entities on Combating Money Laundering and the Financing of Terrorism and Proliferation (hereinafter, the “Policy”) sets forth the basic standards, principles and requirements applicable to internal controls designed for combating money laundering and the financing of terrorism and proliferation.

1.2. This Policy is based on recommendations and requirements of the Financial Action Task Force (FATF).

1.3. The principal goal of this Policy is to lay down standards for effective internal controls designed for combating money laundering and the financing of terrorism and proliferation and aimed at reducing the risk that VEB.RF, VEB.RF Entities and their employees may be involved in transactions associated with money laundering and the financing of terrorism and proliferation.

1.4. The provisions of this Policy shall apply to VEB.RF and VEB.RF’s Entities that conduct transactions involving cash or other assets and are deemed under the laws of the country of their incorporation to be within the purview of the legislation on combating money laundering and the financing of terrorism and proliferation.

2. BASIC TERMS, DEFINITIONS AND ABBREVIATIONS

2.1. VEB.RF: State Development Corporation VEB.RF, established by the Russian Federation with the status, business purposes, functions and powers governed by Federal Law No. 82-FZ of 17 May 2007 “On State Development Corporation VEB.RF”, other federal laws and associated regulations of the Russian Federation;

2.2. VEB.RF’s Entity(ies): any corporate entity(ies) in relation to which VEB.RF has corporate (member) rights and obligations or exercises founder rights, determines the principal areas and priorities of activities, defines policies on risk management and idle cash (liquidity) management, provides financial and guarantee support, and has any holdings other than those arising out of VEB.RF’s investment or export projects (transactions) or subordinated loans and in relation to which either of the following conditions is fulfilled: VEB.RF has a majority equity holding (in excess of 50%) or VEB.RF approves the decision to establish a non-profit organisation as a juridical person;

2.3. VEB.RF/VEB.RF’s Entity manager: the sole executive body/deputy sole executive body/chairman of the collegial executive body/member of the collegial executive body of VEB.RF/VEB.RF’s Entity in charge of supervising the organisation of CML/FT&P activities in accordance with bylaws of VEB.RF/VEB.RF’s Entity;
2.4. VEB.RF/VEB.RF’s Entity senior management: the Supervisory Board of VEB.RF/the highest governing body of VEB.RF’s Entity in accordance with Federal Law No. 82-FZ of 17 May 2007 “On State Development Corporation VEB.RF”/the charter documents of VEB.RF’s Entity;

2.5. CML/FT&P: combating money laundering and the financing of terrorism and proliferation;

2.6. ML/FT&P: money laundering and the financing of terrorism and proliferation;

2.7. CML/FT&P internal controls: activities/a set of measures designed to identify operations (transactions) subject to mandatory (special) control and any other ML/FT&P-related transactions involving cash or other assets;

2.8. ICR: the internal control rules designed for CML/FT&P and approved as a comprehensive document or a set of documents that govern CML/FT&P activities of VEB.RF/VEB.RF’s Entities in accordance with national legislation;

2.9. CML/FT&P Officer: the special officer responsible for complying with and implementing the ICR within VEB.RF/VEB.RF’s Entity;

2.10. special division: the division of VEB.RF/VEB.RF’s Entity responsible for complying with national legislation on CML/FT&P and reporting to VEB.RF/VEB.RF’s Entity manager or to the CML/FT&P Officer in accordance with national legislation and bylaws of VEB.RF/VEB.RF’s Entity;

2.11. customer: any corporate entity or individual, including an individual entrepreneur, or any foreign unincorporated entity receiving services from an organisation that conducts transactions involving cash or other assets (an organisation that conducts financial transactions), including services from an organisation that conducts financial transactions under a written contract for financial transactions;

2.12. customer’s representative: any person that transacts in the name and on behalf or for the account of the customer under a power of attorney or contract or pursuant to an authorised government agency’s or a local government’s resolution or in accordance with laws, and a corporate entity’s sole executive body/the chairman of a corporate entity’s collegial executive body;

2.13. beneficial owner: any individual who ultimately, whether directly or indirectly (through third parties), owns or controls the customer. Whether any person qualifies as the beneficial owner shall be determined in accordance with national legislation;

2.14. beneficiary: any person that receives benefits from the customer. Whether any person qualifies as the beneficiary shall be determined in accordance with national legislation;

3. GOALS AND PRINCIPLES OF CML/FT&P

The basic goals and principles of CML/FT&P at VEB.RF/VEB.RF’s Entities are as follows:

3.1. ensure compliance with national legislation on CML/FT&P;
3.2. apply CML/FT&P to all operations (transactions) in accordance with national legislation;
3.3. protect VEB.RF/VEB.RF Entities from taking illegally gained proceeds;
3.4. prevent VEB.RF/VEB.RF Entities from being involved in ML/FT&P;
3.5. enter into contractual relationships only with financial institutions that implement CML/FT&P measures;
3.6. develop CML/FT&P internal controls, define their special role in the existing internal control system and implement other internal organisational measures related to CML/FT&P;
3.7. ensure that the VEB.RF/VEB.RF’s Entity manager supervises the organisation of CML/FT&P activities and the compliance of the ICR with national legislation on CML/FT&P;
3.8. involve employees of VEB.RF/VEB.RF Entities, irrespective of their position and within their area of responsibility, in implementing CML/FT&P internal controls in accordance with the ICR;
3.9. carry out ML/FT&P risk management;
3.10. maintain the effectiveness of CML/FT&P internal controls at a level sufficient for ML/FT&P risk management;
3.11. ensure the independence of the CML/FT&P Officer in accordance with national legislation and bylaws of VEB.RF/VEB.RF’s Entity;
3.12. forbid CML/FT&P measures from being disclosed to the customer and any other persons unless otherwise provided for in national legislation on CML/FT&P;
3.13. produce regular reporting on CML/FT&P in accordance with national legislation and the ICR.

4. UNIFORM BANS AND RESTRICTIONS

4.1. For the purposes of CML/FT&P, VEB.RF/VEB.RF’s Entities are prohibited under national legislation from:
4.1.1. allowing any anonymous holders to open and operate any bank (deposit) accounts, i.e. any opening individuals, corporate entities or foreign unincorporated entities failing to provide the documents or information required to be made available for their identification, and allowing any holders to open and operate any bank (deposit) accounts under an alias (false name);

4.1.2. allowing the customer to open any bank (deposit) accounts without the personal presence of the opening individual or the customer’s representative unless otherwise provided for in national legislation;

4.1.3. entering into and maintaining relationships with any non-resident banks that fail to have a permanent governing body in the country of their incorporation;

4.1.4. entering into any bank (deposit) account agreement with the customer if the customer or the customer's representative fails to provide the documents or information required, under national legislation, to be made available for the identification of the customer or the customer’s representative unless otherwise provided for in national legislation.

4.2. VEB.RF/VEB.RF’s Entities may:

4.2.1. refuse to enter into any bank (deposit) account agreement with the customer in accordance with the ICR if it is suspected that the purpose of such agreement is to conduct ML/FT&P-related transactions;

4.2.2. refuse to execute the customer’s instructions to conduct any transaction as and where provided for in national legislation;

4.2.3. terminate (repudiate) any bank (deposit) account agreement as and where provided for in national legislation.

5. BASIS OF THE CML/FT&P SYSTEM

5.1. With the aim of implementing CML/FT&P internal controls, VEB.RF/VEB.RF’s Entities shall create CML/FT&P systems designed to accomplish the goals of national legislation and internal regulatory documents on CML/FT&P.

5.2. The CML/FT&P system is based on the ICR, other internal regulatory documents on CML/FT&P, and a set of special-purpose software tools and applications that make up an integrated software and hardware system helping to implement CML/FT&P measures as required.

5.3. The ICR, together with the principles and measures contained therein, forming CML/FT&P internal controls and used by VEB.RF/VEB.RF’s Entities to protect against or promptly identify ML/FT&P risk shall be implemented by the operations function (the 1st
line of defence), the CML/FT&P Officer/special division (the 2nd line of defence) and internal control and internal audit (the 3rd line of defence).

5.4. The ICR shall be formulated and approved by VEB.RF/VEB.RF’s Entities subject to national legislation that ensures compliance by all financial institution and designated non-financial businesses and professions with the FATF Recommendations.

5.5. The ICR shall take account of the business purpose, functions, customer base and organisational structure of VEB.RF/VEB.RF’s Entity, the nature of products (services) provided to the customer, and the level of ML/FT&P risk.

5.6. The ICR shall generally describe the overall structure and elements (levels) of the CML/FT&P system and lay down the principles and mechanisms for the interaction between the elements of the system; shall set out regulations regarding the status, functions, rights and responsibilities of the CML/FT&P Officer/special division and regarding the principles and procedure for its interaction with the VEB.RF/VEB.RF’s Entity manager and divisions; shall contain information concerning the special-purpose electronic technology and special-purpose software used solely to implement CML/FT&P internal controls; shall outline the procedure for the interaction with the customer, including using direct banking technology; shall set forth the procedure for documenting, storing and keeping confidential information (documents) received in the course of implementing the ICR; shall set forth the procedure for involving divisions in implementing the ICR; shall set forth the procedure describing how employees of VEB.RF/VEB.RF’s Entity, including the CML/FT&P Officer, inform the VEB.RF/VEB.RF’s Entity manager, the internal audit function and the internal control function of VEB.RF/VEB.RF’s Entity about identified violations of national legislation on CML/FT&P on the part of the staff; shall specify the CML/FT&P measures required to be implemented by VEB.RF/VEB.RF’s Entity in respect of the customer and the customer’s operations (transactions) in accordance with national legislation; and shall formulate the procedure for the following processes:

5.6.1. customer due diligence;
5.6.2. ML/FT&P risk identification, assessment, monitoring and management;
5.6.3. identification of operations (transactions) subject to mandatory (special) control in accordance with national legislation and operations (transactions) suspected to be associated with ML/FT&P (suspicious transactions);
5.6.4. refusal to execute the customer’s instructions to conduct any transaction;
5.6.5. refusal to enter into any bank (deposit) account agreement;
5.6.6. termination of any bank (deposit) account agreement;
5.6.7. freezing and banned (suspended) use of money or any other assets of persons involved in the financing of terrorism and proliferation;

5.6.8. reports sent to the authorised agency;

5.6.9. staff training in CML/FT&P;

5.6.10. other CML/FT&P measures provided for in national legislation.

5.7. Under the ICR specifying special functions of any divisions and employees in respect of CML/FT&P, the relevant provisions shall be incorporated into the regulations for such divisions, and the responsibilities of employees shall be incorporated into the job descriptions for such employees of VEB.RF/VEB.RF Entities.

6. PARTICULARITIES OF CML/FT&P INTERNAL CONTROLS

6.1. The particularities of CML/FT&P internal controls used by VEB.RF/VEB.RF’s Entities shall be defined by national legislation.

6.2. The effectiveness and adequacy of CML/FT&P internal controls shall generally be evaluated in the following categories:

- corporate governance for the purposes of CML/FT&P compliance, management oversight and transparency;
- principles and procedures;
- know your customer (KYC), customer due diligence (CDD), enhanced due diligence (EDD);
- other previous risk assessments (both at local level and at VEB.RF/VEB.RF’s Entity level);
- management information/reporting;
- data storage and storage length;
- appointment of the CML/FT&P Officer/special division;
- identified and reported suspicious transactions;
- monitoring and control;
- training;
- independent testing and oversight (including the relevant results of internal control or internal audit or any other material facts).

6.3. The ICR formulated in the Russian Federation shall be in compliance with Federal Law of the Russian Federation No. 115-FZ of 7 August 2001 “On Anti-Money Laundering and Combating the Financing of Terrorism” subject to the requirements approved by the Government of the Russian Federation or, in the case of credit institutions, professional securities market participants, insurance undertakings (except
for health insurance undertakings), investment fund managers, mutual funds, private pension funds and unit investment funds, consumer credit cooperatives, microfinance lenders, mutual insurance societies and private pension funds, by the Central Bank of the Russian Federation in consultation with the federal executive authority that implements CML/FT&P measures in accordance with legislation on CML/FT&P.

6.4. VEB.RF/VEB.RF’s Entities may set up the special division and appoint the CML/FT&P Officer whose qualifications and business reputation shall meet the requirements of national legislation.

Unless otherwise required, the CML/FT&P Officer may act in this capacity alongside having other responsibilities, except for the responsibilities of internal audit, provided that the CML/FT&P Officer is not entitled to sign on behalf of VEB.RF/VEB.RF’s Entity any payment documents, accounting records or any other documents causing VEB.RF/VEB.RF’s Entity to exercise and perform any rights and obligations.

6.5. The main functions of the CML/FT&P Officer/special division are as follows:

6.5.1. formulate the ICR;

6.5.2. take decisions in implementing CML/FT&P internal controls, including in relation to transactions subject to mandatory (special) control and suspicious transactions and in respect of the customer that conducts such transactions;

6.5.3. organise and supervise the submission of reports to the authorised agency;

6.5.4. prepare and submit CML/FT&P reports to the VEB.RF/VEB.RF’s Entity manager, the VEB.RF/VEB.RF’s Entity senior management and/or such other governing body of VEB.RF/VEB.RF’s Entity as required under national legislation in accordance with the procedure and within the period set forth in the ICR.

6.6. With the aim of performing the functions entrusted to the CML/FT&P Officer/special division, the CML/FT&P Officer/special division shall have the rights and responsibilities provided for in national legislation.

6.7. Organising CML/FT&P internal controls in the Russian Federation shall be subject to the Russian legal requirements that prohibit bank deposit agreements with bearer deposit notes and that prohibit any corporate entity from opening a bank account without the personal presence of its representative if the credit institution suspects that opening any such bank account is associated with ML/FT&P or if such corporate entity and/or any person authorised to act on its behalf, and/or its beneficial owner (any of its beneficial owners), and/or its member (any of its members), except for a shareholder that is a corporate entity and has a shareholding of more than 25 per cent in the corporate entity opening the bank account, are:
- a person on the list of organisations and individuals alleged to be involved in extremism, terrorism or the proliferation of weapons of mass destruction, or an organisation or individual whose money or other assets are frozen by the interdepartmental coordinating body in charge of combating the financing of terrorism;
- a person found by the credit institution to be subject to the measures contained in paragraphs 5.2 and/or 11 of Article 7 of Federal Law of the Russian Federation No. 115-FZ of 7 August 2001 “On Anti-Money Laundering and Combating the Financing of Terrorism”;
- a person whose details of incorporation are registered as invalid on the Uniform State Register of Juridical Persons.

6.8. VEB.RF/VEB.RF’s Entities shall take measures to prevent any relationships with non-resident banks found to allow accounts with them to be used by any banks that fail to have a permanent governing body in the country of their incorporation.

7. KYC PROCEDURES

7.1. VEB.RF/VEB.RF’s Entities shall accept the customer’s operations (transactions) after identifying the customer, the customer’s representative, the beneficial owner and the beneficiary and identifying the degree (level) of the customer’s risk.

7.2. VEB.RF/VEB.RF’s Entities shall take all necessary measures to implement the FATF’s KYC recommendations making it possible to verify the identity of the customer or the customer’s representative and requiring that the following conditions should be fulfilled:

7.2.1. VEB.RF/VEB.RF’s Entities collect all the information necessary to conclude that the customer or the customer’s representative, the beneficial owner and the beneficiary (if any) are identified completely;

7.2.2. VEB.RF/VEB.RF’s Entities understand that the customer does not conduct ML/FT&P-related transactions;

7.2.3. VEB.RF/VEB.RF’s Entities conclude that the money involved in any operation (transaction) are not the customer’s illegally gained proceeds;

7.2.4. VEB.RF/VEB.RF’s Entities check the customer, the customer’s member, the beneficial owner, the customer’s representative and the customer’s management for inclusion on specialised lists of international organisations or individual countries that impose sanctions or restrictions on the customer/country;

7.2.5. VEB.RF/VEB.RF’s Entities understand that the customer acts on the customer’s own behalf or on behalf of third parties.
7.3. For the purposes of identification, VEB.RF/VEB.RF’s Entities shall obtain the information specified in the ICR in respect of the customer, the customer’s representative, the beneficial owner and the beneficiary. For this purpose, the customer, the customer's representative, the beneficial owner and the beneficiary are, inter alia, required to complete questionnaires.

7.4. In the course of identifying the customer, the customer’s representative, the beneficial owner and the beneficiary, VEB.RF/VEB.RF’s Entities shall verify any information received from the customer by using reliable independent source documents, sources, publicly available information systems of government agencies, and databases (databanks) of, for example, Russian and foreign companies offering information products, such as Dow Jones Risk & Compliance (Factiva), Interfax (SPARK, Corporate Information Disclosure Center), Interfax – D&B (DBAI, GRS, KYC reports) and SKRIN.

7.5. VEB.RF/VEB.RF’s Entities shall take reasonable measures to identify the beneficial owner and verify the identity of the beneficial owner. Such measures (for example, obtaining information about the management and ownership structure of the customer that is a corporate entity) shall enable VEB.RF/VEB.RF’s Entities to believe that they know the identity of the beneficial owner.

7.6. The customer is not required to be identified (may be left unidentified) where provided for in national legislation unless VEB.RF/VEB.RF’s Entities learn or suspect that the customer’s activities or individual transaction is associated with ML/FT&P.

7.7. The identification of the customer shall result in VEB.RF/VEB.RF’s Entities understanding the goals and intended nature of the business relationship with the customer, obtaining information on the customer’s business reputation and the customer’s source of funds (if necessary), analysing the business relationship with the customer and examining the operations (transactions) conducted as part of such relationship in order to make sure that such operations (transactions) are consistent with the available information on the customer, the customer’s business activities and the degree (level) of the customer’s risk.

7.8. VEB.RF/VEB.RF’s Entities shall take reasonable measures to find out whether the customer, the beneficial owner or the beneficiary (if any) is a foreign politically exposed person, a domestic politically exposed person or a politically exposed person of an international organisation (PEP).

If the customer is identified as a PEP or a PEP’s family member, the VEB.RF/VEB.RF’s Entity manager or a duly authorised division head of
VEB.RF/VEB.RF’s Entity shall decide in writing on entering into a business relationship or continuing the existing business relationship with the customer.

If VEB.RF/VEB.RF’s Entities enter into a business relationship with a PEP or a PEP’s family member, they shall take the following additional CML/FT&P measures:
- establish the customer’s source of wealth and the customer’s source of funds;
- conduct constant enhanced monitoring of the business relationship with the customer.

7.9. VEB.RF/VEB.RF’s Entities shall, within the period specified in the ICR, update the information obtained from the identification of the customer, the customer’s representative, the beneficial owner and the beneficiary (if any) and update the degree (level) of the customer’s risk. Information on the customer shall also be revised and updated if any changes are detected in the customer’s governing bodies or ownership structure or otherwise as specified in the ICR.

7.10. The results of identification and the updated information obtained from the identification of the customer shall be documented in KYC profile forms. KYC profile forms shall be completed in accordance with the ICR.

8. RISK ASSESSMENT

8.1. VEB.RF/VEB.RF’s Entities shall assess ML/FT&P risk by using a risk-based approach that enables them to implement CML/FT&P measures corresponding to identified risks and distribute their own resources in the most efficient manner.

8.2. The general principles of the risk-based approach are based on the recommendations of the FATF and the Wolfsberg Group and consist in the possibility of using expanded CML/FT&P controls for high risks and using simplified CML/FT&P controls for lower risks. However, simplified measures are not allowed if ML/FT&P is suspected.

8.3. The risk-based approach gives due consideration to types of VEB.RF Entities; types of activity and business conducted by VEB.RF/VEB.RF Entities and exposed to the risk of ML/FT&P; types of customers, products, services and sales channels; particular geographic presences/country risks; and other qualitative factors.

Such factors include, but are not limited to, as follows:
- stability of the customer base;
- integration of IT systems;
- expected growth in the number of accounts/customers;
- expected growth in earnings;
- up-to-date information concerning changes in the staff of the special division;
- confidence in third-party services;
- recent/intended introduction of new products and/or services;
- recent/intended takeovers;
- recently completed projects and initiatives relating to CML/FT&P compliance (for example, corrective measures, corrections or offshoring);
- up-to-date information concerning the use of necessary corrective action;
- national risk assessments.

8.4. The system of ML/FT&P risk assessment for the activities of VEB.RF/VEB.RF Entities generally includes the following types of risk:

8.4.1. the risk that the customer may conduct ML/FT&P-related transactions (the customer’s risk);

8.4.2. the risk that VEB.RF/VEB.RF’s Entities and their employees may be involved in ML/FT&P (the risk of using VEB.RF/VEB.RF’s Entity services for ML/FT&P).

8.5. The customer’s risk shall be assessed in respect of all customers, including customers receiving services from VEB.RF/VEB.RF’s Entities on a one-off basis, unless the customer is not identified in accordance with national legislation or the ICR.

The customer’s risk of ML/FT&P shall be assessed at all stages of services provided to the customer, such as:

- providing the customer with access to services and identifying the customer;
- accepting the customer’s operations (transactions);
- updating information on the customer as required.

8.6. The customer’s risk shall be assessed as a result of analysing the documents and information obtained by VEB.RF/VEB.RF’s Entities from the customer’s identification in respect of the customer and the customer’s activities and as a result of analysing the additional documents and information obtained at the request of VEB.RF/VEB.RF’s Entities, including by comparing the information contained therein with the information available to VEB.RF/VEB.RF’s Entities and by analysing the customer’s operations and transactions.

8.7. In order to assess the degree (level) of the customer’s risk, certain criteria shall be established which may include the country of the customer’s incorporation, the type of the customer’s business, the customer’s reputation, services requested by the customer, the period of the customer’s duration and other factors. The degree (level) of the customer’s risk shall be assessed on the scale applied by VEB.RF/VEB.RF’s Entities.
8.8. In the course of using the risk-based approach for risk assessment and with the aim of managing and reducing the risk that VEB.RF/VEB.RF’s Entities may be involved in ML/FT&P, they shall take the following measures:

8.8.1. identify the customer, the customer’s representative, the beneficial owner and the beneficiary, including collecting additional information on the customer in accordance with the KYC principles;

8.8.2. monitor the customer’s transactions and activities in order to establish that the customer’s transactions shall or may be deemed to be associated with ML/FT&P;

8.8.3. identify and assess ML/FT&P-associated risks inherent in the activities of VEB.RF/VEB.RF’s Entities with due consideration to the nature and size of business;

8.8.4. create and implement controls and procedures designed to effectively manage and reduce the identified risks associated with ML/FT&P;

8.8.5. monitor, improve and (if necessary) expand such controls and procedures.

9. Monitoring of Transactions

9.1. VEB.RF/VEB.RF’s Entities shall monitor the customer’s operations (transactions) in order to identify any operations (transactions) subject to mandatory (special) control and any suspicious operations (transactions) in the customer’s activities.

9.2. Suspicious operations (transactions) shall be identified using the criteria designed to determine whether such operations (transactions) appear unusual, and the list of criteria is not intended to be exhaustive. Such criteria shall be added by VEB.RF/VEB.RF’s Entities at their discretion on the basis of the nature, scale and main areas of the activities of VEB.RF/VEB.RF’s Entities and the customer.

9.3. Whether any operation (transaction) qualifies as suspicious shall be independently determined by VEB.RF/VEB.RF’s Entity based on the available information and documents describing the status and activities of the customer conducting such operation (transaction) and the beneficial owner, along with the customer’s representative, the beneficiary and the customer’s member (if any).

9.4. In order to identify any operations (transactions) subject to mandatory (special) control and any suspicious operations (transactions) in the customer’s activities, VEB.RF/VEB.RF’s Entities shall define the procedure for the interaction of divisions with the CML/FT&P Officer/special division and their authority and functions as systematic measures to verify information on the customer and the customer’s operations (transactions), including the procedure for monitoring and control.
9.5. Particular attention shall be paid to the customer’s operations (transactions) using modern technology that enables remote access to the customer’s accounts.

9.6. If any operation (transaction) meets one of the criteria of suspicious transactions, this shall not provide the basis for the customer’s operation (transaction) automatically qualifying as suspicious but shall serve as the basis for the enhanced verification of documents and information on the customer and the customer’s transaction and activities, including by making enquiries and taking other measures to obtain further information about whether the transaction is consistent with the goals of the customer’s activities and has a legal and economic purpose.

In the course of taking such measures, VEB.RF/VEB.RF’s Entities shall use all possible legally available sources, including external information, such as media outlets, publicly available information systems of government agencies and documents describing the status and activities of the customer, the customer’s representative, the beneficiary, the beneficial owner and the customer’s member.

The time required to carry out enhanced verification shall be specified in the ICR.

9.7. Particular attention is required if the customer conducts suspicious transactions regularly and/or on a large scale. If there are reasonable grounds for such suspicion, measures shall be taken in relation to the customer in accordance with national legislation, such as a refusal to provide the customer with access to direct banking services, including accepting the customer’s instructions signed with the equivalent of the customer’s handwritten signature to conduct transactions in the bank (deposit) account and switching over to accepting the customer’s payment documents only in hard copy form.

9.8. The customer’s activities shall be monitored manually or automatically.

9.9. For the purposes of CML/FT&P, the employees of VEB.RF/VEB.RF Entities involved in conducting any transaction shall not be allowed to take the final decision on how the transaction should qualify.

The final decision on whether or not the customer’s transaction should qualify as suspicious shall be taken by the CML/FT&P Officer. For this purpose, the CML/FT&P Officer’s decision shall be guided by all the available documents and information.

**10. STAFF TRAINING**

10.1. For the purposes of CML/FT&P, VEB.RF/VEB.RF’s Entities shall provide staff training.
10.2. Staff training for VEB.RF/VEB.RF Entities shall include teaching national legislation, regulatory requirements, the ICR and other internal regulatory documents on CML/FT&P, along with:

10.2.1. classification, typical schemes and methods of ML/FT&P; criteria used to determine whether any transactions appear unusual;

10.2.2. CML/FT&P-related responsibilities of employees, including identifying the customer, the customer’s representative, the beneficial owner and the beneficiary, obtaining the necessary documents from the customer, identifying any transactions subject to mandatory (special) control and any transactions suspected to be associated with ML/FT&P, and reporting such transactions to the authorised agency;

10.2.3. sanctions that may be imposed on employees of VEB.RF/VEB.RF’s Entities for failure to comply with national legislation, the ICR or other internal regulatory documents of VEB.RF/VEB.RF’s Entities on CML/FT&P.

10.3. Staff training in CML/FT&P shall also be provided externally and shall include teaching the particularities of CML/FT&P in professional securities trading.

10.4. The training procedure shall be specified by VEB.RF/VEB.RF’s Entities in the ICR in accordance with national legislation. In order to cover a wide range of employees and ensure its timeliness, training shall use different methods, including remote training.

10.5. For the purposes of staff training, VEB.RF/VEB.RF’s Entities shall, jointly with the CML/FT&P Officer, select divisions and employees that shall receive training in CML/FT&P. In this connection, due consideration shall be given to the functions and responsibilities of such divisions and employees. Employees of the divisions responsible for banking operations (transactions), legal support for the activities of VEB.RF/VEB.RF’s Entities, internal audit, internal control, including in relation to CML/FT&P, and security shall receive training on a compulsory basis.

10.6. At the end of training, employees’ knowledge of CML/FT&P shall be tested. The results of training and knowledge tests shall be properly documented (as certificates or other documents) and stored by VEB.RF/VEB.RF’s Entities.

11. STORAGE AND CONFIDENTIALITY OF INFORMATION

11.1. VEB.RF/VEB.RF’s Entities shall document information on CML/FT&P in order to promptly make it available to authorised agencies upon request and, if necessary, find details of an operation (transaction), the amount of an operation (transaction), the currency of payment, the customer’s counterparty etc. Any information
and records relating to CML/FT&P shall be so documented and kept as to be able to be used as evidence in court proceedings.

11.2. Information and documents relating to CML/FT&P shall be kept for the period provided for in the ICR, but at least five years after the end of the business relationship with the customer.

11.3. The following information and documents shall be subject to mandatory storage in hard copy and/or electronic form:

- information and documents obtained from the identification of the customer, the customer's representative, the beneficiary and the beneficial owner;
- accounting records and payment documents (copies thereof);
- KYC profile forms;
- reports sent to the authorised agency, including reports on transactions subject to mandatory (special) control and suspicious transactions;
- documents relating to operations (transactions) that provide the basis for reports on transactions subject to mandatory (special) control and suspicious transactions;
- documents relating to an analysis that provides the basis for deeming the customer’s transaction suspicious;
- documents related to communication with the customer and third-party organisations and institutions;
- other documents and software applications provided for in national legislation on CML/FT&P and the ICR.

11.4. For the purposes of CML/FT&P, VEB.RF/VEB.RF’s Entities shall keep confidential:

- information obtained from the identification of the customer, the customer's representative, the beneficiary and the beneficial owner, including information on the customer’s accounts (deposits) and transactions, and information contained in KYC profile forms;
- information concerning the measures taken by VEB.RF/VEB.RF’s Entities in respect of the customer in determining whether its activities meet the criteria of potential ML/FT&P;
- information made available to the authorised agency in relation to the customer's transactions involving cash or other assets;
- other information and documents provided for in the ICR.

11.5. Information shall be kept confidential using, inter alia, the following methods:
11.5.1. incorporate in the ICR the provisions that govern the procedure for storing information and documents on CML/FT&P;

11.5.2. restrict access to information and documents on CML/FT&P unless such access is directly required by employees’ functions and falls within their responsibility;

11.5.3. ban the following acts:
- inform the customer and any other persons about CML/FT&P measures carried out by VEB.RF/VEB.RF’s Entities unless otherwise provided for in national legislation;
- inform any employees who are not involved in conducting (supporting) any operation (transaction) about the contents of the documents and information obtained from the customer or the customer’s representative and revealing potential activities associated with ML/FT&P (unless otherwise provided for in the ICR).

12. FINAL PROVISIONS

12.1. This Policy is subject to revision and updating as may be necessary, including in the event of changes in national laws, international practices, standards and recommendations relating to CML/FT&P. This Policy shall be amended by approving a restated version hereof.

12.2. In all matters not covered by this Policy, national legislation and bylaws of VEB.RF/VEB.RF’s Entity shall apply.