

**THE VTB BANKING GROUP CONSOLIDATED POLICY
ON THE PREVENTION OF MONEY LAUNDERING
AND TERRORIST FINANCING**

CONTENTS

GENERAL PROVISIONS	3
DEFINITIONS	3
GENERAL PRINCIPLES AND COORDINATION WITHIN THE VTB BANKING GROUP	4
REPORTING AND ANALYSIS	4
MAIN RESPONSIBILITIES	4
AMLO STATUS AND RESPONSIBILITIES	5
AML/CFT PROCEDURES	6
CUSTOMER DUE DILIGENCE	6
<i>Identification requirements for new personal customers</i>	<i>6</i>
<i>Politically Exposed Persons (PEPs)</i>	<i>7</i>
<i>Identification requirements for corporate customers</i>	<i>7</i>
<i>Identification requirements for trusts, foundations and similar entities</i>	<i>8</i>
<i>Identification requirements for financial institutions</i>	<i>8</i>
<i>Further information about the non-bank customer</i>	<i>9</i>
<i>Updating customer files</i>	<i>10</i>
MONITORING CUSTOMER ACTIVITY	10
RISK-BASED APPROACH	11
REPORTING PROCEDURES	13
CONFIDENTIALITY	13
RECORDS KEEPING	13
TRAINING OF PERSONNEL	14
CLOSING PROVISIONS	15

GENERAL PROVISIONS

Financial institutions run legal, regulatory, reputational and as a consequence financial risks if they are used as vehicles for money laundering and terrorist financing.

The VTB Banking Group Consolidated Policy on Prevention of Money Laundering and Terrorist Financing stipulates the general framework of internal AML/CFT control within the VTB Banking Group in order to mitigate the above mentioned risks.

When implementing AML/CFT controls Members of the VTB Banking Group follow national laws and regulations and this Policy. National laws and regulations prevail if in conflict with any of the provisions of this Policy.

DEFINITIONS

AML/CFT	-	Anti-Money Laundering/Combating the Financing of Terrorism;
AMLO	-	Anti-Money Laundering Officer - an employee of the Bank, who is responsible for the Bank's compliance with AML/CFT internal control rules and for reporting to the Authorized body;
Authorized body	-	National body (bodies) receiving suspicious transactions reports and other reports sent by the Bank in accordance with national AML/CFT laws and regulations;
Bank or Member of the VTB Group	-	JSC VTB Bank or any other bank, where JSC VTB Bank holds more than 50% (a subsidiary);
Customer	-	Any individual or entity who seeks to enter or has already entered into a business relationship, or conducts a one-off transaction, with the Bank, as principal or as an agent for someone else;
FATF	-	Financial Action Task Force, an intergovernmental body which sets standards, develops and promotes policies to combat money laundering and terrorist financing;
KYC	-	Know Your Customer;
National laws and regulations	-	Acts of law and regulations or guidance of national authorities which regulate/supervise AML/CFT activities of the Bank;
Politically Exposed Persons (PEPs)	-	Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, their immediate family members or persons known to be close associates of such individuals.
The VTB Banking Group	-	The banking group, which consists of JSC VTB Bank and its subsidiary banks;

GENERAL PRINCIPLES AND COORDINATION WITHIN THE VTB BANKING GROUP

Wishing to unite their efforts in preventing involvement in money laundering or terrorist financing activities, the Members of the VTB Banking Group agree to:

- follow general approaches in establishing and maintaining AML/CFT internal control systems mentioned in this Policy,
- tailor their own internal AML/CFT procedures based on national laws and regulations and on this Policy using the highest AML/CFT standards and best practices applied in the VTB Banking Group,
- take mutual actions to mitigate risks relating to money laundering or terrorist financing in the VTB Banking Group,
- coordinate their efforts when elaborating measures aiming to prevent money laundering or terrorist financing,
- assist each other in solving problems relating to the functioning of AML/CFT internal control system or arising in connection with the implementation of AML/CFT internal control rules on a case by case basis.

In accordance with the FATF Recommendations the principles used by financial institutions to prevent money laundering should be also applied to branches and majority owned subsidiaries particularly those located in countries which do not fully comply with the FATF recommendations, are considered to have inadequate AML standards, insufficient regulatory supervision or present a greater risk of corruption, terrorist financing or crime.

REPORTING AND ANALYSIS

In order to ensure adherence to general principles of AML/CFT internal controls within the VTB Banking Group, to maintain the soundness of AML/CFT system and to assess AML-related risks on a consolidated basis, the Banks forward information about the implementation of the AML/CFT rules and procedures to JSC VTB Bank quarterly.

JSC VTB Bank is responsible for analyzing the reports and other information relating to the functioning of AML/CFT internal controls in the Banks and for preparing consolidated reports to the management of the VTB Banking Group on the effectiveness of the VTB Banking Group AML/CFT strategy and existing money laundering/terrorist financing risks.

JSC VTB Bank is further responsible for elaborating and presenting to other Banks any possible changes and improvements to AML/CFT procedures, which can be of mutual interest and use.

MAIN RESPONSIBILITIES

When establishing and maintaining AML/CFT systems the Banks presume, that:

- they cannot contract out of their regulatory responsibilities, and therefore they remain responsible for their AML/CFT systems and controls,

- the responsibility for the establishment and maintenance of effective AML/CFT systems and controls rests with the senior management of the Bank,
- each Member of the VTB Banking Group has a AMLO appointed by the senior management of the Bank, or as otherwise provided by the national laws and regulations. The AMLO of JSC VTB Bank is informed about a newly appointed AMLO.
- all staff should be fully aware and understand their legal and regulatory responsibilities and obligations with regard to money laundering and terrorist financing activities,
- the senior management receives regular and timely information of the Bank's money laundering/terrorist financing risks effectiveness of the Bank's AML/CFT rules,
- the Banks have internal AML/CFT documents approved by the country supervisory authorities (if necessary), including:
 - customer due diligence and monitoring customer's activities procedures,
 - risk management policies and risk profile in relation to money laundering and terrorist financing and application of those policies,
 - reporting procedures and data protection clauses,
 - record keeping provisions,
 - confidentiality provisions,
 - staff training procedures,
- the internal AML/CFT documents are regularly revised in order to follow the developments in national AML/CFT regulations, the emerging of new products and/or other changes in the Bank's business profile.

AMLO STATUS AND RESPONSIBILITIES

The AMLO of the Bank is a person with adequate seniority and experience having the authority to act independently in carrying out his responsibilities.

The AMLO is responsible for the Bank's compliance with the national AML/CFT laws and regulations and this Policy and ensures that all staff abide by the internal AML/CFT rules and procedures.

The AMLO is further responsible for organizing the procedure of reporting to the Authorized body. It is also his responsibility to respond promptly to any reasoned request for information made by this body, national supervisory or law enforcement authorities.

The AMLO reports annually to the senior management of the Bank on the effectiveness of the Bank's AML/CFT strategy and existing money laundering/terrorist financing risks. This information may also be brought to the notice of the AMLO of the JSC VTB Bank.

AML/CFT PROCEDURES

CUSTOMER DUE DILIGENCE

The Banks take necessary measures to be reasonably satisfied that their customers are who they say they are, as well as to understand that there is no legal barrier to providing them with the product or service requested.

The Banks should take necessary measures to recognize the persons (individuals and legal entities) to whom financial sanctions of national or international bodies apply in order to refrain from entering into a business relationship or conducting a one-off transaction with such persons.

The identity of a prospective customer is not verified in cases provided by the national laws and regulations unless the Bank knows or suspects that a proposed relationship or a one-off transaction involves money laundering or terrorist financing.

The Banks also take reasonable measures to establish, whether the customer is acting for another person or entity and to identify persons to whose advantage the customer acts, except in situations specifically exempted by national laws and regulations.

The Banks refrain from opening accounts for anonymous customers.

Satisfactory identification of the customer takes place as soon as reasonably practicable after first contact between the Bank and the customer. Business could be conducted before satisfactory identification evidence has been obtained only in exceptional cases allowed by national laws or regulations and approved by the management of the Bank as appropriate. In such circumstances, Banks' risk management procedures require controls to be placed over the extent of the relationship entered into, or any funds held under the relationship, until verification has been completed.

In identifying a customer, the Bank obtains a range of information from the customer and verifies this information (or some of it) through the use of reliable, independent source documents, data or information.

Identification requirements for new personal customers

In identifying a natural person, the Bank obtains the following information:

- full name,
- residential address,
- date and place of birth,
- identification documents,
- other information required by national laws and regulations.

The obtained information is verified either on the basis of a document (documents) produced by the customer, or electronically by the Bank (if such a possibility exists under national regulations), or by a combination of both. Where business is conducted face-to-face, the Bank employees have to require originals of any documents involved in the verification and takes copies (where possible). Where it is not possible to take copies of original documents, a file note is made confirming what original documents were sighted to evidence the customers' identity.

Documentary verification of customer's identity is accomplished only on the basis of documents considered as evidences of identity by national laws and regulations.

If identity is verified electronically, this should be on the basis of the customer's full name, date of birth and other criteria, set by national laws and regulations.

Politically Exposed Persons (PEPs)

As regards Politically Exposed Persons, in addition to the standard evidence obtained about an individual the Banks:

- determine, using a risk-based approach, whether a customer is a PEP;
- obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;
- take reasonable measures to establish the source of wealth and source of funds of such customers; and
- conduct enhanced ongoing monitoring of the business relationship.

New and existing customers may not initially meet the definition of a PEP. The Banks should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure.

Identification requirements for corporate customers

The Banks take necessary measures to ensure that the Bank fully understands the company's legal form, structure and ownership, and obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

The Banks obtain the following information in relation to the legal entity concerned:

- full name,
- registered number,
- registered address in country of incorporation,
- business address, place of central management and administration,
- list of administrative bodies and all directors (or equivalent),
- other information required by national laws and regulations.

It is a part of the Banks' procedures to know the names of all beneficial owners of non-personal customers holding 20% of capital or more. However, if national laws and regulations require to identify beneficial owners holding less than 20% or the Bank's assessment of the money laundering or terrorist financing risk presented by the customer is high, it may be decided to verify the identities of beneficial owners holding less than 20%.

Corporate customers that are listed on a regulated market are publicly owned and generally accountable. After satisfying itself that the customer is a publicly quoted company, there is no need of

further steps to verify identity of the customer over and above obtaining the standard evidence mentioned above, if national laws and regulations permit so.

The Banks have to verify the identity of the intermediary and, if the intermediary acts for another, the identity of the underlying customer with the exceptions (if any) made by national regulations.

For operational purposes, the Bank should have a list of those authorized to give instructions for the movement of funds or assets, along with an appropriate instrument authorizing one or more directors (or equivalent) to give the Bank such instructions. The identities of individual signatories need only be verified on a risk-based approach unless the national laws and regulations provide that all authorized signatories should be identified.

Identification requirements for trusts, foundations and similar entities

In addition to the standard evidence obtained about corporate customers the Banks obtain the following information in respect of trusts, foundations and similar entities:

- nature and purpose of the trust, foundation or similar entity,
- country of establishment,
- name and address of any protector or controller,
- other information required by national laws and regulations.

The Banks identify all trustees, settlors, founders, beneficiaries and other persons who have authority to operate an account or to give the Bank instructions concerning the use or transfer of funds or assets following the identification procedure for natural persons or legal entities as the case may be.

The Banks take appropriate steps to be reasonably satisfied that the person the Bank deals with is properly authorized by the customer and is who he says he is.

Identification requirements for financial institutions

When establishing correspondent relations with banks the following elements are considered to be appropriate:

- full name and registration details (registered number and date of registration),
- the jurisdiction where the bank is incorporated (headquartered) and where its operating unit wishing to maintain the relationship with the Bank conducts its business, registered and business addresses,
- the legal form, ownership and executive management of the bank (including information about existence of any PEP in the executive management or ownership structure),
- the types of financial products and services the bank is offering and the markets these products and services are offered to,
- the types of products and services the bank wishes to obtain by establishing correspondent relations,
- general information about the bank's history,

- AML/CFT measures applied by the bank.

Unless national laws and regulations as well as internal procedures of the Bank provide otherwise, before establishing a relationship with a bank the Bank forwards AML Questionnaire to a bank where the risk assessment of money laundering for the bank or country where that bank is domiciled is considered high. As a supplementary tool in obtaining information on a bank the use of Due Diligence Repository of Bankers Almanac (www.bankersalmanac.com) is recommended.

The Banks do not establish correspondent relationships with financial institutions that have no AML/CFT controls. This rule applies to foreign financial institutions incorporated in Non Cooperative Countries and Territories defined by FATF.

The Banks do not establish relationships with shell banks or with institutions acting on their behalf.

If a bank obtaining correspondent banking services provides itself such services to other financial institutions, reasonable steps should be taken to understand the business of financial institutions which receive such services from the customer bank.

The detailed identification and verification procedures for new financial institutions may vary depending on the country of incorporation of the financial institution, if national laws and regulations permit so. However, as a general rule, the Banks should have documentary evidence of:

- the existence of the institutions they intend to establish relationships with,
- a license or other evidence, which confirms that the institution is centrally regulated/supervised in the home country by the regulatory body,
- any other information as required by national laws and regulations.

Further information about the non-bank customer

In order to exercise a risk-based approach more thoroughly, it is recommended that additional information is obtained to the standard evidence which is obtained for the verification of the customer's identity, including some or all of the following:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- whether the expected business be transacted for own or not only for own account (fiduciary business),
- initial and ongoing source(s) of wealth or income (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the relationship between signatories and beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship;
- the purpose and reason for opening the account or establishing the relationship.

In practice, under a risk-based approach, it is not appropriate to know customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Banks' information demands need to be proportionate, appropriate and discriminative.

The Banks should hold a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, as well as of those who seek a product or service carrying a higher risk of being used for money laundering or terrorist financing purposes.

Updating customer files

It is strongly recommended within the VTB Banking Group, that the Banks take steps to ensure that they hold appropriate up-to-date information on their customers. In order to keep the information about customers up to date, the Banks review and update existing customer records not less frequently than once every three years. The review and updating for high-risk customers is performed at least once a year. In addition, a review and update of the customer's records could be performed, if considered necessary, when a transaction of significance takes place (i.e. renewal of facilities, opening of a new account), or when any changes occur in customer's regulatory status, ownership structure, risk profile, etc.

MONITORING CUSTOMER ACTIVITY

Having regard to:

- the general requirement to establish appropriate procedures of internal control for the purposes of forestalling and preventing money laundering/terrorist financing and
- the requirement to report knowledge or suspicion of possible money laundering/terrorist financing and to report cases falling under mandatory control transactions (in some jurisdictions), the Banks establish and maintain an appropriate approach to enable them to detect transactions or activity that may raise suspicions for money laundering or terrorist financing as well as to detect mandatory control transactions (in appropriate jurisdictions).

In addition to carrying out customer due diligence and exercising KYC policies, the Banks monitor customer activity with a view to identify, during the course of a relationship, unusual activity. If unusual events cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions throughout a relationship helps to give greater assurance that the Bank is not being used for purposes of money laundering or terrorist financing.

The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- the reports on these transactions and/or activities are reviewed promptly by the authorized person(s); and
- appropriate action is taken if the findings of such further examination so warrant.

Monitoring can be executed:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or

- after the event, through some independent review of the transactions and/or activities that a customer has undertaken.

In both cases, unusual transactions or activities are flagged for further examination.

The monitoring procedures include types of customer's transactions, the profile of the customer, comparison of the customer's activity and profile with that of a similar, peer group of customers.

It is also recommended, that the Banks have systems and procedures to deal with customers who have not had contact with the Bank for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, in order to be able to identify future reactivation and possible unauthorized use.

In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume, size and character of transactions with customers, in the context of the assessed customer and product risk.

Monitoring systems can be manual and/or automated. However, it is essential to keep the staff of the Banks alert, since such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognize transactions that do not seem to make sense for that customer, cannot be automated.

RISK-BASED APPROACH

By implementing a reasonably designed risk-based approach, the Banks identify the criteria to measure and mitigate potential money laundering and terrorist financing risks.

To assist the overall objective to prevent money laundering and terrorist financing through the VTB Banking Group and its Members, a risk-based approach:

- recognizes that the money laundering/terrorist financing threat varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows senior management to apply its own approach to the Bank's procedures, systems and controls and arrangements in particular circumstances; and
- helps to produce a more cost effective AML/CFT system.

A risk-based approach takes a number, or all, of the following steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the Bank:

- identify and assess the money laundering and terrorist financing risks that are relevant to the Bank;
- design and implement controls to manage and mitigate the assessed risks;
- monitor and improve the effective operation of these controls.

In identifying and assessing the above mentioned risks, the Banks determine and use their own criteria considering that the general trends of assessment include:

- customer base;
- products and services offered by the Bank;
- delivery channels used by the Bank;
- geographical areas of the Bank's operation.

As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures:

- to verify the customer's identity;
- to collect additional KYC information about the customer, and
- to monitor his transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

The Banks decide, on the basis of their assessments of the risks posed by different customer/product combinations, the level of verification that is applied at each level of risk presented by the customer. Consideration is given to all the information gathered about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer. Certain jurisdictions are recognized internationally as having inadequate Anti-Money Laundering standards, laxing regulatory supervision or presenting a greater risk of corruption, crime or terrorist financing. Others, such as many members of FATF, have more robust regulatory environments, which present lower risks.

To assess that risk mitigation procedures and controls are working effectively, the Banks' internal AML/CFT procedures will need to be kept under regular review with the following aspects to consider:

- appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;
- reviewing ways in which different products and services may be used for money laundering/terrorist financing purposes, and how these ways may change;
- adequacy of staff training and awareness;
- monitoring compliance arrangements (such as internal audit/quality assurance processes or external review);
- the balance between technology-based and people-based monitoring and assessing systems;
- capturing appropriate management information;
- upward reporting and responsibility;
- effectiveness of liaison between AML Compliance department of the Bank and other Bank departments; and
- effectiveness of the liaison with regulatory, supervisory and law enforcement agencies.

Risk management generally should be regarded as a continuous process, carried out on a dynamic basis. The Banks therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review. It is recommended that the Banks revisit their assessments at least annually. Details of the assessment and any resulting changes should be included in the AMLO's annual report.

REPORTING PROCEDURES

There are two types of transactions, which are to be reported to the Authorized body:

- transactions subject to mandatory control according to national laws and regulations, and
- transactions and activities, in respect to which knowledge, suspicion, or reasonable grounds for knowledge or suspicion exist, that a person is engaged in money laundering, or terrorist financing.

Following the differences in national legislations, the Members of the VTB Banking Group have dissimilar scope of responsibilities with regard to reporting transactions and activities.

However, the following core obligations are part of reporting procedures of all the Banks:

- all staff participates in raising information about transactions, which are subject to reporting procedures,
- the Bank's AMLO considers all internal reports on transactions subject to reporting procedures,
- the Bank's AMLO makes an external report to the Authorized body within the period of time stipulated by the law, or as soon as it is practicable, if there are no special provisions in national legislation,
- suspicious approaches are also reported, even if no transaction takes place,
- all actions in respect of transactions subject to reporting procedures are to be documented and retained under regular review,
- the details of transactions which are subject to reporting procedures and all correspondence exchanged with the authorities in relation to these transactions are documented,
- the external reports to the Authorized body should contain as much information about the customer, transaction or activity as is determined by national laws and regulations.

CONFIDENTIALITY

The information about customers and their transactions obtained in the course of fulfilling AML/CFT internal control is considered as confidential.

The employees of the Banks should not disclose to other persons the AML/CFT ways and means employed by the Bank.

The "tipping off" is strictly prohibited.

RECORDS KEEPING

The Banks keep records, including:

- customer information,
- transactions,
- internal and external reports about suspicious and mandatory control transactions,
- AMLO annual (and other) reports,
- information not acted upon,
- training and information about the effectiveness of training, containing, in particular:
 - dates AML/CFT trainings were given,
 - the nature of the training,
 - the names of the staff who received training; and
 - the results of the tests undertaken by staff, where appropriate,
- compliance monitoring containing, in particular:
 - reports by the AMLO to senior management; and
 - records of consideration of those reports and of any action taken as a consequence.

Records concerning customer identification and transactions are kept as evidence of the work that the Banks have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

Records of identification evidence are kept for a minimum period of five years after the relationship with the customer has ended unless the national laws and regulations provide for a longer period.

The date the relationship with the customer ends is the date:

- a one-off transaction, or the last in a series of linked transactions, is carried out; or
- the business relationship ended, i.e. the closing of the account or accounts.

Records of all transactions reported to the Authorized body are kept for a minimum period of five years from the date of the transaction unless the national laws and regulations provide for a longer period.

Records of all internal and external reports are retained for a minimum of five years from the date the report was made unless the national laws and regulations provide for a longer period.

Besides, the Banks make and retain records of actions taken under the internal and external reporting requirements. When the AMLO has considered information or other material concerning possible money laundering or terrorist financing, but has not made a report to the Authorized body, a record of the material that had been considered is kept as well.

TRAINING OF PERSONNEL

One of the most important controls over the prevention and detection of money laundering or terrorist financing is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of mandatory control transactions and unusual activities or transactions which may prove to be suspicious.

Therefore, the Banks' relevant staff should be given appropriate training in order to be aware of:

- the legislation relating to money laundering and terrorist financing,
- the documents relating to the prevention of money laundering and terrorist financing issued by regulating and supervising authorities,
- the Bank's policies and procedures of internal control in relation to the prevention of money laundering and terrorist financing,
- the potential effect on the whole VTB Banking Group, the Bank, its employees personally and on its customers, of any breach of the AML/CFT rules,
- their responsibilities in connection with the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering or terrorist financing, etc,
- the identity and responsibilities of the AMLO.

It is recommended that the Banks' relevant staff and in particular employees engaged in customer acceptance, customer servicing, or in settlements receive training at least every 18/24 months or more frequently if circumstances or national regulations require it. Following national laws and regulations, the circle of employees being trained may be broadened.

Extra trainings are given, if AML/CFT laws and regulations or the Bank's policies and procedures in relation to the prevention of money laundering and terrorist financing have materially changed.

Relevant employees are trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions need different training, tailored to their particular function. This may involve making them aware of the importance of the KYC requirements for money laundering prevention purposes, and of the respective importance of customer identification procedures, obtaining additional KYC information and monitoring customer activity.

The necessity of AML/CFT training is considered as well where staff move between jobs, or change responsibilities.

CLOSING PROVISIONS

This Policy is subject to approval of the Steering Committee of the VTB Banking group. After this Policy is approved by the Steering Committee of the VTB Banking group the Members of the VTB Banking group shall use its provisions, which do not contradict with their national laws and regulations, for tailoring and improving their AML/CFT internal control rules.

This Policy is done in Russian and English. In case of divergent interpretation the Russian text shall prevail.