BANK ESKHATA

"Approved"
by the Supervisory Board of
OJSC "Bank Eskhata"
Minutes No.08/2024
dated April 30, 2024

POLICY P-002:2024

ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION IN OJSC "BANK ESKHATA"

(VERSION 08)

Effective as of 06/05/2024

Table of Content

Chapter 1. General Provisions

1.1 This Policy has been developed on the basis of the Law of the Republic of Tajikistan "On Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation of Weapons of Mass Destruction" (hereinafter the Law), other regulatory legal acts of the Republic of Tajikistan and requirements developed in this area by such generally recognized international organizations as Organization for Economic Cooperation and Development (OECD), the Financial Action Task Force on Money Laundering (FATF), the Basel Committee on Banking Supervision, as well as taking into account the recommendations, requirements and practices of leading international financial organizations.

1.2 The Policy applies to all structural units of the Bank and its subsidiaries. The Bank applies the requirements of this Policy to its shareholders, customers, counterparties, and persons involved in joint projects with OJSC "Bank Eskhata" (i.e., contractors, consultants, suppliers, etc.).

1.3 Compliance with the requirements of this Policy applies to all employees, customers, partners and counterparties of the Bank as well as other persons involved in joint projects with the Bank who carry out transactions with cash and other property.

1.4 The provisions and principles approved in this Policy are fundamental in the development of the Bank's internal regulatory documents governing the processes of establishing business relations and interaction with customers, correspondent banks and partners of the Bank.

1.5 The Compliance Risk Department is the responsible unit that ensures the proper implementation of this Policy within the Bank.

Chapter 2. Key Terms and Abbreviations

The Bank- OJSC "Bank Eskhata"

Shell Bank - A shell bank is a bank that has no physical presence in a country where it is incorporated and licensed and is not affiliated to any regulated financial group that is subject to effective consolidated supervision.

Beneficial Owner – natural person (s) who owns (own) directly or indirectly (through third parties, including through a chain of ownership) (has (have) predominant stake in the capital of the customer) or actually control(s) the customer, or an individual on whose behalf or interests an operation (transaction) is carried out, as well as an individual(s) controlling a legal entity or a foreign legal entity.

Immediate Relatives – a spouse, children, parents, brothers, sisters, adoptive parents, adoptive children, as well as other persons who, according to the information provided or otherwise available, jointly reside and have common household with a public official on a permanent basis;

Business relations – relations between a customer and the Bank based on an agreement to provide financial or other services, including carrying out an operation (transaction).

Compliance Risk Department is a structural unit of the Bank responsible for the internal control over the compliance of the Bank's activity to the requirements of the legislation of the Republic of Tajikistan, regulatory legal acts of the NBT, internal rules and procedures of the Bank, as well as AML/CFT/ PWMD issues;

FMD - Financial Monitoring Department under the National Bank of Tajikistan;

Customer Identification - a set of measures to verify the identification data of the customer

(customer's representative);

Property (Funds) - assets of any kind, tangible or intangible, movable or immovable, regardless of the way of their acquisition as well as legal documents or instruments in any form, including electronic or digital ones, certifying the title to or interest in such assets, including bank loans, traveller's cheques, bonds, bills of exchange, letters of credit, virtual assets and etc.;

Customer - an individual or a legal entity, as well as a foreign legal entity serviced by the Bank;

Compliance Ambassador - an employee of the Bank's structural unit appointed by the Chairperson of the Management Board responsible for identification of compliance risks and meeting AML/CFT/ PWMD requirements in the structural unit of the Bank;

Compliance Risk - the probability of losses resulting from non-compliance by the Bank and its employees with the requirements of the legislation of the Republic of Tajikistan, regulatory legal acts of the Authorised Body, internal regulatory documents of the Bank governing the procedures for providing services and conducting transactions in the financial market by the Bank, as well as the legislation of foreign countries that affects the activities of the Bank;

Confidential Business - activities where it is not possible to identify the ultimate beneficial owners, the type of transactions/activities carried out and other information required to comply with the requirement of the legislation of the Republic of Tajikistan;

Legalization of Proceeds of Crime (Money Laundering) - execution of financial operations or other transactions with cash, securities or other property, if it is known that such property represents proceeds of crime, for the purpose of concealing or disguising the source of receipt of this property or for the purpose of assisting a person involved in the commission of the predicate offence so that he/she can evade responsibility for his/her actions, as well as concealing or disguising the true nature, location, method of disposal, movement, rights to the property or its belonging, as well as the acquisition, possession, use or disposal of such property.

International Sanctions are sanctions recognised by the Republic of Tajikistan, in accordance with international treaties or other regulatory legal acts of the Republic of Tajikistan as well as sanctions that may have a material effect on the Bank's operations, its reputation or expose the Bank's customers and partners to the risk of loss of their assets;

NBT – the National Bank of Tajikistan;

National List is a list of individuals and legal entities that are labelled by Tajik authorities as having links to terrorism and extremism. It is provided by the Authorised Body.

Unusual Transaction – a transaction that contains possible signs and criteria of unusual nature and not typical for a particular customer's transaction, as well as any transactions that, according to the judgment of the financial monitoring department specialists, may be carried out for AML/CFT/PWMD purposes;

SB – the Supervisory Board of OJSC "Bank Eskhata"

UNO – United Nations Organisation

Responsible Person of the Bank is a special officer appointed by the Supervisory Board of the Bank, who is responsible for development and arrangement of the implementation of the internal control rules on AML/CFT/PWMD at the Bank and this person is a compliance-controller on sanctions as well.

FMD - Financial Monitoring Division of the Compliance Risk Department;

PO - public official - one of the following individuals:

a) **foreign public official** - a person who performs or has performed significant public or political

functions in a foreign country (heads of state or government, high-ranking political figures, high-ranking officials of government, courts, armed forces, law enforcement, fiscal or other public authorities, high-ranking officials of state-owned enterprises, as well as leaders and activists of political parties);

b) **national public official** - a person who holds or has held in the past a public office of state power, or a political office of state service, or an administrative office of state service of the highest category in the Republic of Tajikistan in accordance with the Register of public offices of the Republic of Tajikistan, approved by the President of the Republic of Tajikistan, or equivalent public offices in the armed forces, law enforcement or other state bodies of the Republic of Tajikistan

c) **public official of an international organization** - an official of an international organization who is or has been entrusted with an essential function of that international organization (directors, deputy directors and members of the management or board of directors of an international organization or other persons of equivalent status in an international organization);

AML/CFT/ PWMD - anti-money laundering and combating the financing of terrorism and proliferation of weapons of mass destruction.

Suspicious Transaction and Operation - an operation or transaction with property (funds), including an attempt to execute an operation or transaction, regardless of its amount, in respect of which there is a suspicion that it may be related to money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction;

Internal Control Rules on AML/CFT/PWMD – Rules of control on anti-money laundering and combating the financing of terrorism and proliferation of weapons of mass destruction adopted in OJSC "Bank Eskhata";

Management Board - the Management Board of OJSC "Bank Eskhata";

RT – the Republic of Tajikistan

Risk is a set of threats, vulnerabilities to ML/FT/ PWMD and related consequences for the state, state bodies and (or) the Bank;

Sanction – an element of a legal norm that asserts certain restrictions related to the conduct of transactions and the establishment of adverse consequences if these restrictions are not met.

Structural Unit - units of the Bank and its branches that carry out transactions with customers and establish relations with counterparties and partners within the requirements of the legislation of the RT;

Authorized Body – a body for combating money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, which is determined in accordance with the Law of the RT On Anti-Money Laundering, Combating the Financing of Terrorism and Financing the Proliferation of Weapons of Mass Destruction;

Financing the Proliferation of Weapons of Mass Destruction (PWMD) is the direct or indirect provision or collection of funds with the purpose of their full or partial use, or with the knowledge that they will be used in the illegal development, production, acquisition, storage, transportation, shipment or transfer to another person in possession of nuclear, neutron, chemical, biological (bacteriological), climatic, and other types of weapons of mass destruction prohibited by international treaties, as well as the transfer to any non-nuclear-weapon country of source or special fissionable material or technology known to be capable of being used for the production of weapons of mass destruction, or the provision

to any person of other types of weapons of mass destruction or components necessary for their production prohibited by international treaties;

Financing of Terrorism - direct or indirect provision or collection of funds, for the purpose of their full or partial use or in the knowledge that they are to be used by an individual terrorist or terrorist group (organization), or for the purpose of financial support for an individual terrorist or terrorist group (organization) or for the organization, preparation and commission of crimes of terroristic nature, notwithstanding that such funds were not actually used to commit the listed crimes, as well as financing of an individual terrorist or terrorist group (organization), even if it is not related to a specific terrorist act(s) or to finance the travel of persons travelling to a country other than their country of residence or citizenship for the purpose of committing, planning, preparing or participating in the commission of terrorist acts, or for the training of terrorists, or receiving such training;

FATF – The Financial Action Task Force on Money Laundering, an intergovernmental organization that sets AML/CFT/PWMD standards, develops and implements policies on anti-money laundering, combating the financing of terrorism and financing of the proliferation of weapons of mass destruction;

OFAC – (**Office of Foreign Assets Control**) - U.S. Treasury's Office of Foreign Assets Control, a financial intelligence and enforcement agency of the U.S. Treasury Department. It administers and enforces economic and trade sanctions in support of U.S. national security and foreign policy objectives;

SDN List (Specially Designated Nationals and Blocked Persons List) – a list managed by OFAC, it contains legal entities and individuals involved in prohibited activities, including the proliferation of weapons of mass destruction, terrorism, drug trafficking, as well as violating human rights and freedoms;

SSI List (Sectoral Sanctions Identification List) is a list that identifies persons operating in sectors of the Russian economy identified by the U.S. Secretary of the Treasury as prohibited to deal with;

UNSC – The United Nations Security Council;

Chapter 3. Goals and Objectives of the AML/CFT/PWMD Policy

3.1 The main goals of this Policy are:

3.1.1 Prevention of involvement of the Bank in activities related to ML/FT/PWMD.

3.1.2 Ensuring compliance of the Bank's activities as well as the activities of each of its employees with the legislation of the RT and internal regulatory documents of the Bank in the area of AML/CFT/PWMD;

3.1.3 Compliance with the requirements of international treaties, as well as with the recommendations of international organizations on AML/CFT/PWMD, including FATF within the limits established by the relevant legislation of the RT;

3.1.4 Laying the groundwork for the internal control system development and the adoption of internal regulatory documents of the Bank on measures for risk management associated with the possible involvement of the Bank in ML/FT/PWMD processes.

3.1.5 Ensuring compliance of the Bank's legal framework with international standards on AML/CFT/ PWMD issues in the part that does not contradict the legislation of the RT.

3.1.6 Ensuring the compliance of Bank with international economic sanctions and minimising compliance risk in the Bank's activities related to non-compliance with international economic sanctions, implementing the best international practices and decisions of the SB on sanctions compliance.

3.2 The main objectives of this Policy are:

3.2.1 Prevention of ML/FT/PWMD activities at the Bank by the persons who have business relations with the Bank.

3.2.2 Development and implementation of effective measures to detect and prevent ML/FT/PWMD by the Bank's customers and beneficial owners to minimize the following risks:

3.2.2.1 risk of damage to the Bank's business reputation;

3.2.2.2 risk associated with violation of AML/CFT/PWMD legislation;

3.2.2.3 risk associated with the violation of AML/CFT/ PWMD legislation of foreign countries where the Bank conducts payments and transfer operations, as well as transactions of the Bank's customers through foreign credit financial institutions;

3.2.2.4 risk of non-compliance with sanctions, including international sanctions.

3.2.3 Ensuring employees of the Bank comply with the requirements of this Policy as well as them applying its requirements in practice, taking into account the following features:

3.2.3.1 participation of employees in the implementation of internal control procedures on AML/CFT/PWMD, regardless of the position held;

3.2.3.2 compliance with bank secrecy requirements and preventing disclosure of information revealed in the course of internal control procedures for AML/CFT/PWMD purposes;

3.2.3.3 preventing the participation or assistance of the Bank's employees in ML/FT/PWMD processes;

3.2.3.4 ensuring clear allocation of functions between the structural units of the Bank, including branches (unit responsible for AML/CFT/PWMD) to exercise effective control over compliance with internal procedures on AML/CFT/PWMD;

3.2.4 Ensuring the organization and implementation of the internal control system for the Bank's compliance with international economic sanctions.

Chapter 4. Organization of Internal Control for AML/CFT/PWMD Purposes

4.1 Authority system

4.1.1 The following authority system has been approved for the operation of the AML/CFT/FROMS system:

- The SB;
- Compliance and Risk Management Committee under the SB;
- Chairperson of the Management Board;
- Management Board;
- Compliance Risk Department;
- Responsible Person of the Bank;
- Compliance Ambassador of the branch /Structural unit

4.1.2 The scope of the SB authority includes:

4.1.2.1 approval of this Policy, as well as other internal regulatory documents of the Bank that determine focus area of the Bank in the area of AML/CFT/PWMD;

4.1.2.2 review of reports on compliance risks accepted by the Bank and proposed measures to minimise the risks of involving the Bank and its employees in ML/FT/ PWMD processes;

4.1.2.3 control over the Bank's implementation of internal control measures for AML/CFT/PWMD purposes and assessing their effectiveness.

4.1.2.4 appointment of a Responsible person/persons of the Bank (compliance controller on AML/CFT/PWMD) and control over their activities to ensure compliance with AML/CFT/PWMD legislation.

4.1.3 Authority of the Compliance and Risk Management Committee in the area of AML/CFT/PWMD includes:

4.1.3.1 ensuring the reliability and effectiveness of the internal control system, as well as coordinating activities and providing methodological support in these directions;

4.1.3.2 evaluating the effectiveness of the Bank's internal control and risk management systems, as well as developing proposals on these and related issues;

4.1.3.3 providing recommendations to the SB regarding the approval of the appointment and removal of the Head of the Compliance Risk Department and the Responsible person of the Bank;

4.1.3.4 Preliminary review and recommendation of internal regulatory documents defining the activities of the Bank in the area of AML/CFT/PWMD for approval of the SB;

4.1.3.5 Review of reports submitted to the Committee on the AML/CFT/PWMD system effectiveness.

4.1.4 The authority of the Chairperson of the Management Board includes:

4.1.4.1 overall coordination and control over the effectiveness of the Compliance risk management system established at the Bank;

4.1.4.2 ensuring the promotion of the compliance culture at the Bank;

4.1.4.3 conducting external and internal communications regarding the provisions of this Policy, its importance, binding nature and need for its enforcement;

4.1.4.4 ensuring that employees who have properly fulfilled their responsibility to comply with the requirements of the Policy are protected from retaliation, discrimination or unwarranted disciplinary measures.

4.1.5 The authority of the Management Board includes:

4.1.5.1 ensuring the integration of AML/CFT/PWMD functionality into the Bank's business processes;

4.1.5.2 making decisions on projects submitted for consideration, taking into account the provisions of this Policy and the identified compliance risks;

4.1.5.3 reviewing of compliance risk reports for AML/CFT/PWMD purposes.

4.1.6 The functions of the Compliance Risk Department within AML/CFT/PWMD framework are defined in the Bank's internal regulatory documents, the Department:

4.1.6.1 arranges the development of this Policy, the Internal Control Rules on AML/CFT/PWMD as well as other internal regulatory documents on AML/CFT/PWMD issues and their submission for

approval, ensuring the implementation of the requirements established by legislation of the RT, FATF recommendations, UNSC resolutions;

4.1.6.2 monitors compliance of the employees of the Bank with AML/CFT/ PWMD laws and regulations.

4.1.6.3 makes decisions on suspending/blocking transactions when exercising internal control for the purposes of AML/CFT/ PWMD, including customer transactions that are suspected of being carried out for the purposes of ML/FT/PWMD;

4.1.6.4 identifies, evaluates, monitors and controls and anticipates risks of ML/FT/PWMD in the activities, projects and transactions of the Bank and its subsidiaries, and provides recommendations to the Bank's management bodies on minimising them;

4.1.6.5 provides training and advice to staff on the issues of AML/CFT/ PWMD;

4.1.6.6 coordinates of the activities of the Bank and its subsidiaries on the issues of risk management of money laundering and financing of terrorism;

4.1.6.7 improves the regulatory framework and management system of AML/CFT/PWMD to increase their efficiency and ensure their consistence with the Bank's goals and objectives;

4.1.6.8 provides a response to requests of Authorised body, other regulatory and law enforcement authorities, partners, counterparties and correspondents of the Bank on AML/CFT/PWMD issues;

4.1.6.9 supports the inspections and inquiries of Authorised body, other regulatory and law enforcement authorities, internal and external audits, partners, counterparties and correspondents of the Bank on AML/CFT/PWMD issues;

4.1.6.10 reviews and evaluates ML/FT/PWMD risks as part of the overall risk management system in accordance with the Bank's strategy and objectives;

4.1.6.11 develops AML/CFT/PWMD reporting system and provides information to the Bank's management bodies in the following order:

- submission of the approved reporting form to the Management Board-at least once a month;
- submission of the approved reporting form to the SB, the Compliance Committee - at least once a quarter.

4.1.7 The reports to be submitted shall include, but are not limited to the following items:

4.1.7.1 the results of customer risks monitoring analysis and assessing the degree of exposure of the Bank's products (services) to ML/CFT/ PWMD risks at the Bank's level (as a whole) and per its structural units;

4.1.7.2 recommendations on preventive measures to minimize ML/CFT/PWMD risks, including deadlines for the implementation of the proposed measures;

4.1.7.3 recommendations for the elimination of violations and shortcomings in the Bank's activity identified during the compliance control process, including AML/CFT/PWMD issues;

4.1.7.4 on the measures implemented to eliminate the violations identified by the internal audit unit and/or the Authorized Body based on the results of audits of the effectiveness of the Bank's compliance risk management system, including AML/CFT/PWMD issues, and their results, or on the failure to implement such measures, if any.

4.1.7.5 existing issues hindering the successful implementation of the internal control system

4.1.8 The powers and functions of the Responsible Person of the Bank are determined by the Internal Control Rules on AML/CFT/PWMD and the related job description. The exclusive authority of the Bank's Responsible Person includes:

4.1.8.1 ensuring the implementation of this Policy, Internal Control Rules on AML/CFT/PWMD and other internal regulatory documents of the Bank related to the activity of the Bank in the area of AML/CFT/PWMD and their compliance with the legislation of RT;

4.1.8.2 monitoring of the Bank's employees on the implementation of the laws and regulations on AML/CFT/PWMD;

4.1.8.3 arranging trainings for employees on issues related to AML/CFT/PWMD;

4.1.8.4 analysis of suspicious and unusual transactions;

4.1.8.5 arranging investigation of transactions/operations on AML/CFT/PWMD issues, if required;

4.1.8.6 arranging investigation of unusual transactions, if required

4.1.8.7 reviewing internal reports on suspicious and unusual transactions for the accuracy of their compilation;

4.1.8.8 monitoring of timely submission and registration of reports on suspicious transactions/ operations to the Authorized Body on AML/CFT/PWMD;

4.1.8.9 providing instructions to the Bank's employees on non-disclosure of information to the customer regarding AML/CFT/PWMD measures;

4.1.8.10 acting as a contact person with Authorized Body in the area of AML/CFT/ PWMD, against law enforcement bodies, as well as with any other competent authorities regarding prevention, detection, investigation, or compliance with AML/CFT/PWMD standards;

4.1.8.11 ongoing study of national and international changes in the area of AML/CFT/PWMD and submission of proposals for consideration of the SB and Management Board to bring the activity and internal regulatory documents of the Bank in line with new requirements.

4.1.8.12 ensuring the collection, control, processing and analysis of information on the requirements of the UNSC resolution;

4.1.8.13 ongoing monitoring of the updating of sanctions lists and the introduction of new sanctions programmes;

4.1.8.14 informing the SB about introduction of sanctions significantly affecting the Bank's activities;

4.1.8.15 ensuring sanctions compliance, including international sanctions

4.1.8.16 developing procedures for screening new and existing customers, counterparties, partners against sanctions lists

4.1.8.17 ensuring inspections (testing) of the AML/CFT/PWMD compliance system, including:

- inventory of lists on the Bank's CBS;
- procedures for risk level assignment;
- processes for identifying transactions subject to mandatory control, suspicious transactions, as well as timely submission of notification to the Authorised Body about such transactions.
- proper operation of sanctions control system at the Bank
- other areas of AML/CFT/PWMD at the Bank.

4.1.8.18 ensuring that a remedial action plan is drawn up to address the findings of the above-mentioned inspections;

4.1.8.19 organising monitoring of the Bank's involvement in confidential business transactions;

4.1.8.20 making decisions to terminate business relationships with customers, partners, or counterparties or restricting their access to Bank's services in cases set out in this Policy.

4.1.9 The Chairperson of the Management Board appoints Compliance Ambassador who is responsible for compliance with the Internal Control Rules on AML/CFT/PWMD after completing a special training course on AML/CFT/PWMD. Functions of Compliance Ambassador:

4.1.9.1 cooperation with Financial Monitoring division of the Compliance Risk Department;

4.1.9.2 ensuring implementation of this Policy and internal documents on AML/CFT/PWMD within their own unit;

4.1.9.3 assistance to the Responsible Person of the Bank in control of compliance with this Policy and procedures on AML/CFT/PWMD issues by the structural unit;

4.1.9.4 the matter of trainings coordination and raising awareness of the structural unit employees on the requirements of this Policy and procedures on AML/CFT/PWMD issues;

4.1.9.5 ensuring full and timely collection of information on suspicious transactions and its submission to the Financial Monitoring division within its unit;

4.1.9.6 other functions defined in job descriptions and internal regulatory documents.

4.1.10 The authorities and functions of the Bank's structural units related to AML/CFT/PWMD are defined by the Bank in its internal regulatory documents.

4.2 Lines of defence in the internal control system on AML/CFT/PWMD

4.2.1 Units initiating transactions with Counterparties are the first line of defence of the Bank for detecting and preventing ML/FT/PWMD. At the same time, the heads of structural units are responsible for the appropriate arrangement and implementation of internal control in the administrated structural unit. To ensure the effective implementation of the Internal Control Rules on AML/CFT/PWMD in the first line of defence, a Special Branch Officer responsible for AML/CFT/PWMD issues is appointed in the structural units of the Bank, who is responsible for compliance with the above-mentioned Rules.

4.2.2 Compliance Risk Department presents the second line of defence and it is responsible for identifying, assessing, controlling and reporting about such compliance risks the relevant management bodies of the Bank. Structural units of the Bank ensure ML/FT/PWMD is identified and the Bank is protected during the accounting, processing and control of transactions.

4.2.3 The Internal Audit Department provides the third line of defence through an independent assessment of the effectiveness of the internal control system in the area of AML/CFT/PWMD.

4.3 Principles of the organisation of the internal control system in the area of AML/CFT/PWMD

4.3.1 The Bank considers the money laundering and the financing of terrorism as unacceptable phenomena in its activities, which are completely and unconditionally prohibited. The Bank carries out transactions in such a way that the accepted compliance risks were identified, assessed and were at the lowest possible and acceptable level for the Bank. At the same time, since it is usually impossible to

completely exclude the identified risks, their acceptance at the approved level does not mean that the Bank considers Prohibited Practices as permissible.

4.3.2 When developing the internal control system in the area of AML/CFT/ PWMD, the Bank is guided by the following principles:

4.3.2.1 expresses its unequivocal condemnation of terrorism in all its forms and declares that it is unacceptable to use the Bank and its services in illegal transactions, including money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction;

4.3.2.2 recognizes the importance of compliance of the Bank's activities and each of its employees with the legislation, ethical standards and internal regulatory documents of the Bank;

4.3.2.3 recognizes the importance of compliance of this Policy with regulatory requirements and international practice;

4.3.2.4 participation of all structural units and employees of the Bank in the internal control process and the organization of internal control as a daily activity at all levels of management;

4.3.2.5 internal control coverage of all directions of activities and business processes and regulation of internal control procedures in all areas and business processes of the Bank;

4.3.2.6 implementation of internal control on an ongoing basis (continuity).

4.4 General requirements for the organization of internal control in the area of AML/CFT/PWMD

4.4.1 **Internal Control Rules on AML/CFT/PWMD**.

4.4.1.1 In order to implement internal control in the area of AML/CFT/PWMD, the Bank develops Internal Control Rules including but not limited to:

1) AML/CFT/PWMD system programme;

2) customer, customer's representative and its beneficial owner identification programme;

3) ML/CFT/PWMD risk management programme;

4) programme for identifying transactions in customer activities that are subject to mandatory control and suspected of being carried out for of ML/CFT/ PWMD purposes;

5) documenting data and information programme;

6) programme for the organisation of the Bank's activities on refusal of acceptance for service and executing orders for conducting transactions/operations;

7) programme on determining the procedure for applying measures to freeze (block) the customer's funds or other property;

8) programme on training and instruction of employees in the area of AML/CFT/PWMD;

9) internal control audit programme on AML/CFT/PWMD.

10) sanctions compliance programme

4.4.1.2 The Internal Control Rules on AML/CFT/PWMD establish a unified approach to identify transactions of customers (their representatives) and beneficial owners at the Bank by creating and

maintaining databases, analysing suspicious transactions, the procedure for notifying of violations of the legislation of the RT on AML/CFT/PWMD by the employees of the Bank, and also, they ensure methodological unity and coordinated functioning of information systems in the area of AML/CFT/PWMD;

4.4.1.3 The Internal Control Rules on AML/CFT/PWMD are mandatory for all employees of the Bank.

4.4.10 **Requirements for employees on conducting transactions and providing customer service**:

4.4.10.1 identification of banking transactions that are more vulnerable in the area of AML/CFT/ PWMD;

4.4.10.2 carrying out (within the competence) identification and review (due diligence) of customers on a risk-based approach and entering into business relations only with those customers whose due diligence confirms their legal status, legality and legitimacy of their activities. The due diligence of customers (their representatives) and beneficial owners is carried out at the Bank in accordance with the Internal Control Rules on AML/ CFT/PWMD;

4.4.10.3 identification (within the scope of competence) of transactions subject to financial monitoring, as well as those suspected of being (attempted to be) for ML/FT/PWMD purposes);

4.4.10.4 identification and verification of the beneficial owner's identity;

4.4.10.5 obtaining information about the purpose and intended nature of the business relations;

4.4.10.6 ensuring that the customer's risk profile is established and periodically updated in accordance with the Bank's internal documents;

4.4.10.7 ensuring AML/CFT/PWMD programme is compliant with risk management;

4.4.10.8 taking measures to identify Politically Exposed Persons among individuals accepted for service who are classified by the Bank as high-risk customers. Such measures include: verifying a customer's affiliation and/or relationship with a PO, family members and immediate relatives; assessing the reputation of a PO for involvement in ML/FT/PWMD cases; establishing business relations with a PO only on the written approval of the Chairperson of the Management Board or his deputy and the Branch Director/ head of the Operations or the division acting on the basis of the power of attorney of the Chairperson of the Management Board; and taking available measures to identify the source of funds of a PO;

4.4.10.9 timely updating of the identification data of customers and their beneficial owners, including updating of “Know Your Customer” questionnaires within the deadlines set out in the internal regulatory documents of the Bank;

4.4.10.10 in accordance with the requirements of the Law of the RT On AML/CFT/PWMD and the regulatory legal acts of the NBT the Bank carries out financial monitoring of transactions with cash and (or) other property and sends data and information about them to the Authorized Body;

4.4.10.11 the Bank implements the necessary measures to identify third parties acting in the interests of customers, as well as to recognize the transaction as suspicious if it is determined that the transaction is carried out on behalf of immediate relatives and/or partners (having business relations) of persons related to ML/FT/PWMD in accordance with the requirements of the legislation of the RT;

4.4.10.12 in order to assess and minimize the risks of customers conducting transactions related to ML/FT/PWMD, the Bank examines customer in the frame of “Know Your Customer” procedure.

4.4.11 **Organization of internal control with correspondence banks**:

4.4.11.1 The Bank implements measures to prevent the use of cross-border bank correspondent relations for ML/FT/PWMD purposes in accordance with the Internal Control Rules on AML/CFT/PWMD.

4.4.11.2 Prior to establishing a correspondent banking relation with the proposed respondent bank, the Bank provides for the following actions:

- collecting information about the proposed respondent bank, the nature of the respondent bank's activities and its structure;
- determining the entity's reputation and the quality of supervision from publicly available information, and whether the organization was the subject of a money laundering or terrorist financing investigation, or of supervisory actions or sanctions related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction recently;
- determination of the availability of a reliable AML/CFT/PWMD control system by the respondent bank;
- identifying and monitoring the use of correspondent accounts that may be used as "transit accounts" for money laundering or terrorist financing. In correspondent relations, which include the maintenance of " transit accounts", the Bank adheres to the following requirements:
  - the customer (financial institutions- respondent) has fulfilled all the typical customer due diligence obligations for those of its customers who have direct access to the accounts of the correspondent financial institution;
  - the respondent financial institution is able to provide the relevant customer identification data upon request to the correspondent financial institution.
- identification of the state where the respondent bank is registered and its placement in the list of states that do not comply with the requirements of the FATF recommendation or do not properly comply with them.

4.4.11.3 in the framework of the implementation of the "Know Your Customer" principle, the Bank conducts an annual survey of Correspondent Banks.

4.4.11.4 The details of the establishment of business relations with respondent banks are regulated in the Bank's internal regulatory documents.

4.5 Requirements for enhanced customer due diligence measures

4.5.1 The following group of customers is subject to enhanced due diligence:

4.5.1.1 high-risk customers;

4.5.1.2 customers with a wide range of activities;

4.5.1.3 customers with large account turnovers;

4.5.1.4 customers who have been accepted for service for six months or less;

4.5.1.5 customers engaged in the gambling business;

4.5.1.6 customers towards whom suspicious transaction reports have been filed with AML/CFT/PWMD Authorised Body in the last six months; customers for whom AML/CFT/PWMD requests have been received from the AML/CFT Authorised Body in the last six months.

4.6 General rules for monitoring of customers and their transactions

4.6.1 Monitoring of customers and their transactions is the responsibility of the structural units of

the Bank as well as FMD.

4.6.2 The Bank is guided by the following customer sampling rules in the process of monitoring customers and their transactions:

4.6.2.1 by assigned risk groups;

4.6.2.2 by type of activity;

4.6.2.3 by the relevance of the monitoring period;

4.6.2.4 by the amount of transactions carried out.

4.6.3 The Bank uses information from the Core Banking System, data obtained during site visits and conducting customer questionnaires, and information obtained from publicly available sources to conduct monitoring.

4.6.4 In the event the monitoring of customers and their transactions by structural units reveals significant ML/FT/PWMD risks, the information shall be reported to the FMD immediately after the risks are identified.

4.6.5 In cases the monitoring of customers and their transactions by the FMD reveals significant ML/FT/PWMD risks, the information shall be reported to the Compliance and Risk Management Committee under the SB immediately after the risks are identified.

Chapter 5. Restrictions on AML/CFT/PWMD Issues

5.1 In the following cases the Bank rejects to enter into business relations, to carry out transactions and it terminates previously established business relations:

5.1.1 a request for opening a current or savings account for individuals and legal entities is submitted without actual participation of the person or without the participation of a representative of the person the account is opened for;

5.1.2 failure to provide the required supporting documents with mandatory data of an individual and/or a legal entity for registration according to the Law;

5.1.3 providing inaccurate information required for conducting due diligence of the customer by individuals and legal entities;

5.1.4 there is information about the Bank customer's participation in ML/FT/PWMD received in accordance with the legislation of the RT;

5.1.5 a request for opening a bank account for anonymous (fictitious) customers, the Bank does not conduct payments and transfers on behalf of customers to such bank accounts;

5.1.6 the Bank refuses to establish and maintain business relations with a customer, a partner or a counterparty or limits their access to certain services of the Bank in cases such business relations entail a high risk of non-compliance with the legislation of the RT, international sanctions, or there is a risk of the Bank being involved in illegal activities or ML/FT/ PWMD processes;

5.1.7 the Bank refuses to establish and maintain business relations with a customer, a partner or a counterparty in case of having reasonable suspicions that the customer, the partner or the counterparty is engaged in illegal activity or participates in ML/FT/PWMD;

5.1.8 the Bank does not establish or maintain correspondent relations with shell banks, as well as with the banks that do not implement measures on AML/CFT/PWMD. The Bank does not establish or maintain correspondent relations with foreign financial institutions that allow shell banks to use their accounts;

5.1.9 the Bank reserves the right to refuse establishing contractual relationships and carrying out transactions involving shell banks;

5.1.10 the Bank implements measures against carrying out transactions with foreign financial institutions that allow shell banks to use their accounts;

5.1.11 The Bank may rely on intermediaries or other third parties for the due diligence of the customer and rely on the measures taken by the latter, provided that conditions exist in accordance with the requirements of the Law of the RT On AML/CFT/PWMD and the regulatory legal acts of the NBT. When engaging intermediaries or other third parties for customer due diligence, the Bank shall assume the responsibility for customer due diligence, as well as take necessary measures to minimise ML/FT/PWMD risks

5.1.12 the Bank does not establish business relations with customers engaged in production of weapons and radioactive substances enrichment for manufacture of weapons of mass destruction, nuclear energy, trading in bitcoins and other cryptocurrencies and tokens, drugs, medical marijuana, cannabis/hemp seeds, illegal substances and goods, human organs, counterfeit goods and forgeries, pirated information content and software, pornography, falsified data, fake academic articles etc., organising unlicensed lotteries, pyramid schemes, hidden/informal or illegal production, casinos, prohibited religious activities, banned literature.

5.2 The Bank adheres to the requirements of sanctions against organizations and persons included in the National sanctions list as persons associated with the financing of terrorism and extremism, and it implements the measures established by the legislation of the RT in the area of AML/CFT/PWMD.

5.3 The Bank checks the customers and counterparties of the customers for matches with the National sanctions list. In case of matches the Bank suspends the transaction and immediately provides the relevant information to the Authorized Body in accordance with the requirements of the legislation.

5.4 The Bank adheres to the requirements of sanctions determined by international organizations in accordance with the treaties, including UNSC resolutions.

5.5 The Bank adheres to the requirements of sanctions against organizations and individuals included in the UNSC list of persons associated with the financing of terrorism and extremism (hereinafter is the UNSC list). The Bank checks the customers and counterparties of the customers for matches with the UNSC list. In case of matches with the list, the Bank suspends transactions and provides information to the FMD.

5.6 As a part of compliance with the requirements of the legislation of the RT and relations with foreign correspondent banks, the Bank is guided by the requirements of international economic sanctions, including those established by the OFAC.

5.7 The Bank adheres to the policy of conducting enhanced due diligence on customers, partners and counterparties registered offshore. For this purpose, links between an offshore company and the country/territory of its incorporation are identified. The Bank does not establish business relationships

with customers, partners and counterparties registered offshore that have no business connection with the country/territory of incorporation.

Chapter 6. Sanctions Compliance

6.1 The Bank implements the necessary measures to identify individuals and legal entities that are sanctioned by the Authorized Body and/or international organizations (UN, EU), and/or specific countries (for example, the United States - OFAC/ SDN List) to prevent the initiation of cooperation and/or conducting single transactions. When establishing business relations with customers, the Bank also checks customers, participants of the transaction, and counterparties for matching with the lists of the FMD, UNSC, EU, and OFAC (SDN List), sanction lists of the EU and other countries. In case of matches with the lists, the procedures provided for in the Bank's internal regulatory documents are carried out.

6.2 The Bank applies enhanced due diligence measures in respect of correspondents, partners and counterparties in case punitive sanctions have been imposed on them, their beneficial owners, officers and subsidiaries for non-compliance with the requirements of AML/CFT/PWMD legislation.

6.3 The Bank has the right to terminate business relations or restrict access to particular banking products if there is verified information about their involvement in processes aimed at circumventing international sanctions.

6.4 The FMD is responsible for monitoring of updating of the list of persons subject to international sanctions and their immediate inclusion into the Bank's CBS.

6.5 International payments of customers are carried out after the Compliance Department checks them for compliance with the legislation in force of the RT, requirements of international sanctions, internal regulatory documents, as well as other requirements. Compliance Risk Department has the right to suspend international payments to carry out mandatory control of the specified payment in accordance with the requirements of the legislation of the RT on AML/CFT/PWMD as well as other requirements specified in this paragraph. If any participants of the payment are on the sanctions lists, the Bank is entitled to reject conducting the payment.

Chapter 7. Responsibility

7.1 All employees of the Bank are responsible for compliance with this Policy. Each employee of the Bank bears responsibility as set forth by the legislation of the RT in the area of AML/CFT/PWMD and the relevant internal documents of the Bank in case of assisting customers and other persons in actions aimed at evasion from financial monitoring procedures.

7.2 Compliance Risk Department of the Bank is responsible for overall monitoring of the Bank’s activities in the area of AML/CFT/PWMD and this Policy implementation.

7.3 Responsible Person of the Bank carries out its activities in accordance with the Rules of Internal Control for AML/CFT/PWMD and the relevant job description.

7.4 The responsible person for ensuring the implementation of this Policy and the Rules of Internal Control for AML/CFT/PWMD at the branches/operations department is the Director of the branch/ Head of the Operations Department.

7.5 The Internal Audit Department of the Bank includes into its annual audit plan compliance with the requirements of this Policy, the relevant laws of the RT and regulatory legal acts of the NBT in the area of AML/CFT/PWMD. Following the results of the audit, the Internal Audit Department submits a report to the SB of the Bank through the Audit Committee.

7.6 The employees of the Bank bear responsibility as set forth by the legislation of the RT and internal documents of the Bank in case of disclosing information to customers and other persons about the facts of providing information about customer transactions to the Authorized Body.

7.7 The Bank's employees should be aware that the submission of information and documents by the subjects of financial monitoring to the Authorised Body for the purposes and in accordance with the procedure provided for by the Law on AML/CFT/PWMD does not constitute the disclosure of official, commercial, banking or other legally protected secrets.

7.8 The Bank's employees should be aware that in case of providing information to the Authorised Body in accordance with the Law on AML/CFT/PWMD, the subjects of financial monitoring and responsible persons, regardless of the results of the communication, shall not bear the responsibility provided for by the legislation of the RT.

Chapter 8. Final Provisions

8.1 This Policy is approved by the SB on the recommendation of the Management Board of the Bank.

8.2 Changes and amendments to this Policy may be introduced only by the decision of the SB and they are put into effect from the day of registration of the minutes of the SB with the decision, unless another time is provided for the introduction of changes and amendments by the SB.

8.3 The responsible AML/CFT/PWMD division is determined by the Compliance Risk Department.

8.4 The content of this Policy is communicated to all employees of the Bank in accordance with the procedure established by the internal documents of the Bank.

8.5 This Policy is reviewed, as required, but at least biennially.

8.6 In the event if certain clauses of this Policy come into conflict with the new requirements as a result of changes in the legislation in force of the RT or international instruments in the area of AML/CFT/PWMD, this Policy is applied to the extent that it does not conflict with the legislation of the RT or international instruments in the area of AML/CFT/PWMD.

Since the entry into force of this Policy in version 08, version 07 of the document approved by the Supervisory Board (Minutes No.05/23 dated 22.02.2023) shall be deemed invalid.