Approved by
Supervisory Board of
CJSC "Spitamen Bank"
№239/2«15» December 2025

In compliance with
the Board of
CJSC "Spitamen Bank"
101/1«10» December 2025

Procedures of anti-money laundering and counter terrorism financing.

Dushanbe 2025

Contents:

1. Introduction

1.1. Procedures of anti-money laundering and counter terrorism financing has been developed based on "Law of Republic of Tajikistan on combating the legalization of criminal proceeds, terrorism financing, and financing of the proliferation of weapon of mass distruction" , AML/CFT Policy of the Bank and other regulatory procedures.

1.2. Current Procedure is applicable to all the branches of the Bank.

1.3. Current Procedure is subject to change upon amendments in law and regulatory instructions related to AML/CFT in Tajikistan.

1.4. Instructions of current Procedure is intended for internal use only.

2. Main principles

2.1. The main principle of enacting current Procedure is to clearly demonstrate the process of dealing with AML/CFT/PWMD related activities.

2.2. Enhancing control over compliance related risks.

2.3. Maintaining employees compliance with AML/CFT/PWMD related activities.

2.4. Maintaining effective and timely relationship with regulatory body with the purpose of AML/CFT/PWMD.

3. KYC procedures

Customer Acceptance/ Rejection

3.1. Acceptance

Bank shall accept only those clients whose identity is established by conducting due diligence/ enhanced due diligence appropriate to the risk profile of the client as set out in other part (s) of this policy.

The bank is prohibited from establishing relationship with the customers given in the "Rejection" sub-point of this article.

3.2. Rejection

The bank has defined several types of customers who have unacceptably high risk and has decided to preclude such customers from establishing a business relationship.

3.2. l. List of customers (natural and/ or legal) not accepted by bank:

l. Client who refrain from providing information about their identity, source of income, purpose of the account opening & other necessary information or any part of it as per the KYC forms;

2. Client who cannot provide mandatory/ required KYC documents as per the account opening checklist considering type of the Client;

3. Client who has been recognized by bank having background of fraud, forgery & other such activities that are against bank's policies;

4. Client with negative media from reliable source;

5. Client engaged in illegal activities (such as human trafficking, drug dealing, fraud, bribery etc.);

6. Client convicted for a crime included in the predicate offences;

7. Organization undertaking military missions, i.e. mercenary missions;

8. Online casino or an online pharmacy;

9. Client dealing with dating or adult entertainment;

10. Issuer or dealer of virtual currency (e.g. Bitcoin) or involved in converting traditional currency in virtual currency or vice versa or provides related services (software providers, payment processing services, card acquirers);

11. Client who fails to provide adequate identification information or disclose its economic operations;

12. Shell banks & companies or bank which deals with shell banks or a shell company;

13. Client who requests/ insists to have accounts in the name of anonymous or fictitious persons or accounts (including secret accounts and numbered accounts) or accounts that do not bear the

complete name of the beneficiary as shown in the identification documents of the Client;

14. Client from a political regime not recognized by the United Nations;
15. Client who is subject to specific sanctions (i.e. UN, OFAC, HM Treasury, OFSI, Internal lists,), including close family members and close associates;
16. An Online Gaming company;
17. An entity operating in the production and/or wholesale trading of nuclear related raw materials, products and services;
18. A non-profit organization / charity or foundation for charity purposes, which is not registered/ licensed;
19. An organization providing armed security services, without license & or permission of ministry of interior affairs;
20. Entities operating in the defense/military industry which are not licensed by competent ministry;
21. A legal entity with a complex structure, where there is no transparent and legitimate economic reason for its complexity;
22. Off-shore Companies;
23. The execution of transactions related to close family members, close associates or related entities (irrespective of % of ownership) of sanctioned entities/ individuals.
24. Unlicensed financial institutions;
25. Clients conducting unconvencional financial transactions outside financial institutions (Havala;
26. Clients engaged in trade of unlicensed products (sale of licensed games or programs without license);

4. Risk Assessment

In this context the risk is defined as "a function of likelihood of occurrence of risk events and the impact of the risk events". The likelihood of occurrence is a combination of threat and vulnerabilities, or in other words, risk events occur when a threat exploits

vulnerabilities. Accordingly, the level of risks can be mitigated by reducing the size of the threats, vulnerabilities or their impact.

In order to establish the banks' exposure to ML/TF and the efficient management of the risk, the bank needs to identify every segment of its business operations where a ML/TF threat may emerge and to assess their vulnerability to that threat. it is necessary that ML/TF risks are constantly identified at all management levels, from the operational level to the executive board, and to include all organizational units of the banks.

An assessment of ML/TF risks proceeds from the assumption that the different products and services offered by banks in business operations or different transactions executed by them, are not equally vulnerable to be misused by criminals. The purpose of a risk assessment is to apply control measures proportionate to the identified risk. This allows the bank to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk.

The process of risk assessment in the Bank has four stages:

i. Identifying the area of the business operations susceptible to ML/TF;
ii. Conducting an analysis in order to assess the likelihood and impact of ML/TF;
iii. Managing the risks;
iv. Regular monitoring and reviewing the risks.

4.1. ML/TF Risk Identification and Analyses

The first step in assessing ML/TF risks is to identify certain risk categories, such as customers, countries or geographical locations, products, services, transactions and delivery channels specific for the bank. depending on the specificity of operations of a bank, other categories could be considered to identify all segments in which ML/TF risk may emerge. The significance of different risk categories may vary from bank to bank, e.g, a bank may decide that some risk categories are more important to it than others.

For the analysis, the bank should make an estimate of the likelihood that these types of risk will misuse the banks for money

laundering and terrorism financing purposes. this likelihood is for instance high if it can occur several times in a year, medium if it can occur once in a year and low if it is unlikely, but not impossible. in assessing the impact, the banks can for instance look at the financial damage from the crime itself or from regulatory sanctions or reputational damages to the banks. the impact can vary from minor if there are only short term or low cost consequences to (very) major when there are high cost and long term consequences that affect the proper functioning of the bank.

5. High Risk Situations Requiring Enhanced Due Diligence

The Bank has identified the following possible factors and potentially higher risk situations that shall attract the application of enhanced customer due diligence:

5.1. High risk situations identified for customer risk factors shall include the following:

i. The business relationship is conducted in unusual circumstances e.g.

significant/unexplained geographic distance between the Bank's branch and the

customer;

ii. Non-resident customers.

iii. Legal persons or arrangements that manage the assets of third parties;

iv. Companies that have nominee shareholders or shares in bearer form;

v. Activities those are cash-intensive or susceptible to money laundering or terrorism financing;

vi. The ownership structure of the company appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company's business;

vii. Business relationships and transactions conducted other than 'face-to face";

viii. Business relationships conducted in or with the high risk countries;
ix. Politically exposed persons ('PEPs') or customers linked to PEPs;
x. High net worth customers or customers whose source of income or assets is unclear;
xi. Businesses/activities identified by the FIU, or the FATF as of higher money laundering or financing of terrorism risk;
xii. Virtual currency related transactions;
xiii. Customer who trade virtual assets as intermediary;
xiv. Customer engaged in trade of economically critical goods;
xv. Customers engaged in trade of goods extracted from the land;
xvi. Customers engaged in trade of duel used goods;
xvii. Customer engaged in production of duel used goods.

5.2. High risk situations identified for country or geographic risk factors shall include the following:

i. Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems;
ii. Countries identified by NBT as high risk;
iii. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations, OFAC, HM Treasury, OFSI, EU;
iv. Countries classified by credible sources as having significant levels of corruption or other criminal activity;
v. Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country;
vi. Countries and regions where the war is happening.

5.3. High risk situations identified for Products, services, transaction or delivery channel risk factors shall include the following:

i. Private banking;
ii. Anonymous transactions;
iii. Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification;
iv. Payment received from unknown or un-associated third parties;
v. Complex trade financing products;
vi. Transactions intended for the purchase of electronics products that can be used as necessary part of military equipment.

6. Low Risk Situations Requiring Simplified Customer Due Diligence

The Bank has identified the following possible factors and potentially low risk situations that shall attract the application of simplified customer due diligence

6.1. Low risk situations identified for customer risk factors shall include the following:

i. Companies listed on a stock exchange and subject to disclosure requirements either by law, or stock exchange rules or other binding Instructions or Regulations which define requirements to ensure disclosure of beneficial ownership;
ii. Public enterprises.

6.2. Low risk situations identified for country or geographic risk factors shall include the following:

i. Countries classified by credible sources, such as mutual evaluation reports, as having effective AML/CFT systems;
ii. Countries classified by credible sources as having a low level of corruption or other criminal activity.

6.3. Low risk situations identified for Products, services, transaction or delivery channel risk factors shall include the following:

i. Financial activity is carried out by a natural or legal person on an occasional or very' limited basis such that there is a low risk of money laundering and terrorist financing and that are provided to a low risk customer for financial inclusion purposes;

ii. Financial products or services where there is a proven low risk of money laundering or terrorist financing which occurs in strictly limited and justified circumstances and it relates to a particular type of financial institution or activity.

7. Account opening Procedure

The bank shall identify and verify the customers of all forms before establishing a relationship. Bank shall apply simplified due diligence, enhanced due diligence or any other measures to identify and verify a customer before establishing the relationship.

Banks relevant department shall have in place proper procedure for account opening. Bank has to obtain complete KYC documents & information prior to account opening, as per the provisions of this policy & relevant procedures issued by compliance department.

7.1. Customer Identification Program

The Bank has designed and implemented customer identification program taking into consideration the risks set out hereinabove. The bank shall collect all the required KYC documents to identify the identity of the customer. In addition to the KYC documents mentioned below the bank shall request for any other additional documents to identify the customer to its satisfaction. The Bank has required the branches/offices to adopt following measures to manage the risks:

a. To obtain additional information on the customer, beneficial owner, beneficiary and transaction;

b. To establish a risk profile on customers and transactions. The customer profile shall be based upon sufficient knowledge of

the customer and beneficial owner(s) as applicable including the customer's anticipated business with the bank and where necessary the source of funds and source of wealth of the customer;

c. To apply enhanced customer due diligence to high-risk customers;
d. To update the KYC information on all customers at least annually;
e. To adopt other measures as may be prescribed by NBT.

7.2. Customer Identification Requirements

Identification requirements shall include the following:

i. The Bank shall not maintain or open an anonymous account or an account in fictitious names;
ii. The Bank shall ensure to know the true identity of its customers including beneficial owners;
iii. Customer due diligence shall be carried out in the following cases:

Before establishing a business relationship with a customer or opening an account.

a. Before carrying out domestic or international wire transfers.
b. Whenever doubts shall exist about the veracity or adequacy of previously obtained customer identification data
c. Whenever there is a suspicion of money laundering or terrorist financing.

7.3. Identification of Natural Person Customers for account opening

For customers who are natural persons the Bank shall verify the identity using reliable, independent source documents, data, or information which shall include the following:

a. Full name, Father's Name including any aliases;
b. Business Name (in case of sole proprietorship);
c. Gender;

d. Copy of National Registration Card/Citizen Scrutiny Card/Passport;

e. Copy of passport along with valid work permit for Nonresidents;

f. Permanent and mailing address;

g. Copy of address proof;

h. Date of birth;

i. Nationality;

j. Occupation;

k. Income and source of income. (In case of income source being from business, copy of business license), (source being rent of property, copy of rent), (source being salary, copy of employment letter/agreement), and any other relevant document to prove thee source of income;

l. Phone number (if any);

m. Email address (if any);

n. Photo.

7.4. Identification of Legal Person Customers for account opening:

For customers who are Legal persons and Legal Arrangements including partnerships, limited liability partnerships and Trusts the Bank shall identify the customer and its beneficial owners, by understanding the nature of its business, and its ownership and control structure.

The Bank shall obtain and verify the information required using reliable, independent source documents, data, or information which shall include the following:

a. Name, legal form and proof of existence of the legal persons;

b. Certificate of Incorporation/License;

c. Location of the principal place of business of the legal person;

d. Identification documents for Shareholders, Directors, individuals, authorized signatories who have authority to open, operate and close the account and Name &

identification documents of relevant persons holding senior management positions;

e. Mailing and registered address of legal person including phone, fax and e-mail id;
f. Nature and purpose of the business;
g. The identity of the ultimate beneficial owner;
h. Address of head office;
i. Other information if necessary.

Identification of other parties having relationship with the Bank involve all mentioned identification process highlighted above, and also include other measures which are not listed above.

8. Enhanced Customer Due Diligence measures

The Bank shall examine, including by seeking additional information from the customer, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. The information to be obtained shall also include information on the nature or reason for the transaction.

Where the risks of money laundering or terrorism financing are higher, the Bank shall conduct enhanced CDD measures, consistent with the risks identified. In particular, the Bank shall increase the degree and nature of monitoring of the business relationship in order to determine whether those transactions or activities appear unusual or suspicious

Enhanced CDD measures that shall be applied for higher-risk business relationships include, but are not limited to the following:

i. Obtaining additional information on the customer e.g. occupation, volume of assets etc. and updating more regularly (at list once in a year) the identification data of customer and beneficial owner;
ii. Obtaining additional information on the intended nature of the business relationship;

iii. Obtaining information on the source of funds or source of assets of the customer;
iv. Obtaining information on the reasons for intended or performed transactions;
v. Obtaining the approval of senior management (CEO & in absence of CEO other members of the management of the Bank) to commence or continue the business relationship;
vi. Assessment of all involved parties of the contract;
vii. Complete information on line of product delivery.

9. Ongoing Monitoring of Customer Transactions

The Bank shall implement systems to monitor on an ongoing basis customer transactions and the relationship with the customer. Monitoring shall include the scrutiny of customer transactions to ensure that they are being conducted in line with the Bank's knowledge of the customer and the customer risk profile and the source of funds and wealth, and the predetermined limits if any, on the amount and volume of transactions and type of transactions. The Bank shall monitor customers' account activity, on a regular basis to be able to establish patterns, the deviation from which might indicate suspicious activity.

After identifying suspicious transactions while conducting monitoring of clients' activities, the Bank does not inform the client about performing financial monitoring and reporting to regulatory body.

10. Termination of Customer Relationship

If the Bank is unable to comply with the CDD required for a customer including, on the basis of materiality and risk in respect of the existing customer then it shall terminate the customer relationship and consider filing a report to the NBT (FIU).

Individual accounts if they are used for business purpose despite multiple reminders/communications, then it shall terminate such individual customer relationship and advice the customer to open Corporate account to route such business transactions.

In case of a customer where multiple STRs are filed, then post filing of 3 STRs the bank can terminate the customer relationship.

High Risk accounts-customers wherein the account is inoperative for a period of 1 year with no transactions, such accounts will be reviewed and the bank shall initiate termination of the relationship to avoid unnecessary regulatory attention.

Where the Bank is unable to verify the identity of the customer and beneficial owner(s), it shall refrain from opening the account or commencing the business relationship or carrying out the transaction. In such cases, the Bank shall consider filing a suspicious transaction report to the NBT (FIU).

Where information is obtained that customer or stakeholder is having relationship with shell companies/shell banks.

If information about involvement of the client in ML/TF/PWMD activities is found.

In case of acquiring information about the customers relationship with banks or shell companies, unlicensed brokers, online casinos, unlicenses trade of precious metals etc.

In case of customer's relationship with individual or entities from the sanctioned lists.

In case of acquiring information about customers cooperation with individual or groups participating in foreign wars.

11. Cross Border Wire Transfers/International Wire Transfers

The Bank while engaging in cross border wire transfers shall include accurate originator and beneficiary information on wire transfers and related messages and ensure that the information remains with the wire transfer or related messaged throughout the payment chain. The information accompanying all wire transfers shall always contain:

a. The full name of the originator;

b. The originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction;

c. The originator's address, or customer identification, or date and place of birth;

d. The name and address of the beneficiary and the beneficiary account number or a unique identification number where such an account or number is used to process the transaction;

e. The Bank shall not add, omit or change the original information provided by customer.

If the Bank is unable to comply with these requirements, it shall not execute the wire transfer and consider submitting a suspicious transaction report to NBT (FIU).

The bank does not change or hide the clients information with the purpose of circumventing sanctions.

In case of absence of sufficient information, such as absence of full remitters and beneficiaries' information, gathering full correct information is required. In the case of not being able to collect full required information, transaction will not be carried out.

The bank establishes relationship only with the parties who abide by FATF recommendations and sanctions requirements.

12. Record Keeping Requirements

The Bank shall maintain records of the following information:

a. Copies of all records obtained through the customer due diligence process under including documents evidencing the identities of customers and beneficial owners, account files and business correspondence, for at least five years after the business relationship has ended or a transaction with a customer who does not have an established business relationship with the bank has been carried out;

b. All records of transactions, domestic and international, attempted or executed for at least five years after:

- the attempt or execution of the transaction;
- the business relationship has ended
- Transaction with a customer who does not have an established business relationship with the bank has been carried out.

c. All other necessary information and documents that bank/ relevant department presumes to be necessary including records related to the staff rewards, records of the trainings events such as; attendances, training materials & certificates of participation, staff attendance records etc. for the period of not less than five years.

13. Final Provisions

13.1. Current Policy shall be effective from the date of its approval.

13.2. In case of non-compliance with the requirements of this Policy by authorized individuals, necessary measures shall be taken against them in accordance with the requirements of the legislation and internal procedures of the Bank.

13.3. At the time of changes to law of AML/CFT, changes in regulatory acts of National Bank of Tajikistan, current Policy will be amended.