СПИТАМЕН БОНК
ШОИСТА ЗИНДАГӢ НАМО!

Approved by
Supervisory Board of
CJSC "Spitamen Bank"
№ 147 «15» 09. 2023

Anti-Money Laundering/Counter Terrorist Financing Policy

Dushanbe 2023

Contents:

1. Background 3
2. Introduction 4
3. Definition of Money Laundering & Terrorist Financing 4
4. Anti-Money Laundering and Combating Terrorist Financing 5
5. AML/ CFT Legal and Regulatory Framework in Tajikistan 7
6. Responsibilities of Top Management 8
7. Responsibilities of Chief Compliance Officer 9
8. Responsibilities of Compliance Department 10
9. Policies and Procedures 11
10. Customer Acceptance/ Rejection 12
11. Risk Assessment 14
12. High Risk Situations Requiring Enhanced Due Diligence 18
13. Low Risk Situations Requiring Simplified Customer Due Diligence 19
14. Account opening Procedure 20
15. Customer Screening Program 23
16. Politically Exposed Persons and risk Measure 24
17. Enhanced Customer Due Diligence measures 25
18. Ongoing Monitoring of Customer Transactions 25
19. Termination of Customer Relationship 26
20. Correspondent Banking Relationship 27
21. Cross Border Wire Transfers/International Wire Transfers 27
22. Some Red Flags or Indicators of STR 28
23. Staff Safety 29
24. New products and business practices 29
25. Internal Policies, Procedures, Systems and Controls 30
26. Record Keeping Requirements 31
27. Staff Training 32
28. Anti-Bribery and Corruption measures 32
29. Final Provisions 32

List of Acronyms

ML/TF	Money Laundering/ Terrorist Financing
AML/ CFT	Anti-Money Laundering/ Combating Financing of Terrorism
FATF	Financial Action Task Force
FIU	Financial Intellige nce Unit
Bank	CJSC Spitamen Bank
KYC	Know Your Customer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
NBT	National Bank of Tajikistan
OFAC	Office of Foreign Asset Control
UNSC	United Nation Security Council
EU	European Union
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
NGO	Non-governmental Organization or Non-Profit Organization

Anti-Money Laundering /Counter Financing of Terrorism Policy

1. Background

In compliance with Tajikistan anti-money laundering & combat terrorist financing law, Tajikistan counter financing of terrorism law, list of suspicious transaction and activities provided by National Bank of Tajikistan, Spitamen bank has adopted a comprehensive approach to manage the risk of money laundering/terrorist financing and has developed an AML/ CFT framework articulated in this policy.2

The policy provides governing principles for managing the AML/CFT and KYC framework, and shall be supported with relevant procedures and methodologies for

identification, assessment, control and monitoring of such risks keeping in check the Bank's business and regulator specific compliance requirements.

The policy aims at managing money laundering and terrorist financing risks and also oversees its implementation besides ensuring that issues arising out of these activities are resolved effectively and expeditiously.

2. Introduction

This policy has been developed in the basis of the provisions of Tajikistan banking law, Tajikistan AML/ CFT laws & regulations, in order to;

- Meet the requirements of concerning laws/ regulation,
- Protect bank & its system from being used by money launderer & terrorist financer &
- Safeguard the integrity of the country's financial system.

This policy at the macro level is an embodiment of the bank's approach to understand, identify, measure, mitigate & manage the risk of money laundering and terrorist financing. It aims at ensuring the availability of adequate procedures that are required to fight money laundering & terrorist financing.

3. Definition of Money Laundering & Terrorist Financing

3.1. Money Laundering:

Money Laundering is the process by which criminals attempt to disguise the true origin of the proceeds of their criminal activities by the use of the financial system so that after a series of transactions, the money, its ownership and the income earned from it appear to be legitimate. According to FATF, money laundering is the processing of criminal proceeds in order to disguise their illegal origin. This process is often achieved by converting the original illegally obtained proceeds from their original form, usually cash, into other forms such as deposits or securities and by transferring them from one financial institution to another using the account of apparently different persons or businesses.

Generally, the money laundering process consists of three "stages":

Placement: The introduction of illegally obtained money or other valuables into financial or nonfinancial institutions.

Layering: Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration: Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

These "stages" are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

3.2. Terrorist financing

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organizations. The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts ; (iil) organizes or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

4. Anti-Money Laundering and Combating Terrorist Financing

Bank is required to establish effective customer due diligence program that is based on the requirement of local laws & regulations as well as international standards & best practices, to prevent money laundering and terrorist financing.

Bank should know the true identity of their customers, detect and examine suspicious transactions, and report any such suspicions to the NBT (FIU). It shall establish its customer due diligence (KYC) procedures & minimum criteria in their CDD program that is to be observed in its customer relationships applying the risk-based approach to be able to demonstrate to the

supervisor how it assesses the risks of money laundering related to its customer relationships and activities, and how it identifies its customers and knows and monitors their transactions and use of services.

4.1. Necessary Steps in AML& CFT

a) Detect

1. Out of pattern transaction Monitoring;
2. Identification of suspicious transactions /Customers;
3. Reporting of suspicious transactions to FIU;
4. Screening of customer accounts at the time of opening new account/data of existing accounts and transactions with list of prescribed entities/individuals under sanctioned lists -UNSC resolutions, OFAC, US, UK, EU Financial Sanctions, and Internal watch-list.

b) Deter

1. Exercising Due Diligence for opening new accounts and dealing with existing customers;
2. Understanding KYC policy;
3. NBT Laws & Regulations and internal Policies on AML /CFT;
4. Guidelines for account opening;
5. Appointment of Compliance Officers;
6. Periodic updating of customer's information (KYC Renewal) ;
7. Regular review of daily transactions;
8. Refuse bank services/active assistance in transactions which in the opinion of the bank are suspected to be associated with money derived from illegal activities.

c) Prosecute

Money laundering offences are prosecuted by government through establishment of Financial Intelligence Unit (FIU) in the NBT with active assistance of government agencies.

5. AML/ CFT Legal and Regulatory Framework in Tajikistan

The existence of legal and regulatory framework to combat money laundering and terrorist financing is the crucial and an integral element of a sound anti money laundering and terrorist financing regime. Financial Action Task Force recommends that countries should criminalize money laundering and terrorist financing with a view to include the widest range of predicate offenses.

Tajikistan AML/ CFT legal and regulatory framework has enabled financial institutions and designated non-financial business and professions inside the country to develop their policies and procedures in fighting money laundering and terrorist financing.

NBT is the primary financial regulator/ financial supervisory authority in the country and operates under the law "On the National bank of Tajikistan".

The basic responsibilities of National bank of Tajikistan are to;

- Formulate, adopt and execute the monetary policy of Tajikistan;
- Formulate, adopt and implement currency policy and Tajikistan currency arrangements;
- Hold and manage the official foreign exchange reserves of Tajikistan;
- Print, mint and issue Tajikistanis banknotes and coins;
- Act as banker and adviser, and as fiscal agent of the State;
- License, regulate and supervise banks, foreign exchange dealers, money service providers, payment system operators, securities service providers, and securities transfer system operators;
- Establish, maintain and promote sound and efficient systems for payments, for transfers of securities issued by the State or NBT, and for the clearing and settlement of payment transactions and transactions in such securities.

The primary objective of the Policy is to prevent our branch network from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. The policy is proposed to serve the following purposes:

i. To prevent criminal elements from using our branches for money laundering activities;

ii. To enable the branches to know/ understand the customers and their financial dealings better which, in turn, would help to manage risks prudently;

iii. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;

iv. To comply with applicable laws and regulatory guidelines;

v. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures;

vi. To prevent the Bank from being exposed to reputational damage and financial loss in relation to non-compliance with applicable AML-CFT standards;

vii. To detect, deter and prevent money laundering, associated predicate offences and terrorism financing;

viii. To protect the integrity of the Bank from illegal activities and illicit fund flows;

ix. To ensure effective monitoring of the measures implemented and decisive actions against ML/TF threats.

This Policy shall be applicable to all the branches/offices of the Bank and shall be read in conjunction with related operational guidelines issued from time to time.

6. Responsibilities of Top Management

The Top Management of the Bank shall be ultimately responsible for ensuring compliance with applicable statutes, regulations, internal policies and guidelines and ethical standards. In case of cross border businesses, the Top Management shall be responsible for ensuring compliance with applicable laws and regulations prevailing in various jurisdictions where the business is undertaken. The Top Management of the Bank shall be responsible for implementation of the Bank's AML/ CFT Policies, procedures and its associated requirements. They shall also be responsible for the adequacy of processes, systems, policies and procedures that would create an appropriate environment for managing AML/ CFT & compliance risks.

The bank's Board of Management is responsible for establishing AML/ CFT & compliance policies that contains the basic principles to be approved by the Board of Supervisors and explains the main processes by which AML/ CFT & compliance risks are to be identified and managed through all levels of the organization.

The compliance department should advise the Board of Supervisors and Board of Management on the bank's compliance with applicable laws, rules and standards and keep them informed of developments in the area. It should also help educate staff about compliance issues, act as a contact point within the bank for compliance queries from staff members, and provide guidance to staff on the appropriate implementation of applicable laws, rules and standards in the form of policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

To be effective, the compliance department must have sufficient authority, stature, independence, resources and access to the Board of Supervisors. Board of Management should respect the independent duties of the compliance friction and not interfere with their fulfilment.

7. Responsibilities of Chief Compliance Officer

The Chief Compliance Officer of the Bank shall be appointed with the recommendation of the Board of supervisors.

The Chief Compliance Officer shall report to the board of supervisors and shall be responsible for ensuring effective implementation of the AML/ CFT & Compliance Policies and procedures, and other compliance initiatives, coordinating the identification and management of the Bank's AML/ CFT & compliance risks and supervising the activities of other Compliance staff.

The Chief Compliance Officer shall assist the Bank's Top Management in managing effectively the AML/ CFT & compliance risks faced by the Bank and would be responsible for providing clarifications on issues or concerns relating to the Bank's AML/ CFT & compliance

policies, guiding o the compliance staff in performance of risk assessments and reviewing the results of the AML/ CFT risk assessments, compliance risk reviews and compliance monitoring and testing programs.

The Chief Compliance Officer shall be responsible for developing and maintaining the AML/ CFT & compliance Policies including the approval/reporting of exceptions thereto, maintaining oversight of the activities of the Compliance department of Bank and implementation of the AML/ CFT & compliance policy and compliance risk management framework across the Bank.

Further, the Chief Compliance Officer shall be responsible for maintaining a relationship with the regulators supervising the Bank and act as the key interface between the Top Management of the Bank and the regulators.

Furthermore; The Chief Compliance Officer shall participate in the discussion between the Bank and the NBT (FIU) if any.

8. Responsibilities of Compliance Department

The Compliance department shall work with the Business Units, Internal Audit, and Legal department to ensure that compliance activities are aligned with business objectives. It would provide an independent and objective perspective on emerging compliance issues. The Compliance staff will have a reporting relationship to the Chief Compliance Officer and would be responsible for implementing the compliance framework across the Bank.

The responsibilities of the Compliance department shall be disseminated via regulatory guidelines/instructions to business units, provide guidance in the implementation of the AML/ CFT & compliance policies and compliance framework to the compliance staff and respond to AML/ CFT & compliance related requests/queries of employees.

The Compliance department shall also be responsible for developing and maintaining the compliance for all regulatory reporting, disseminating the same to the relevant Business Units, monitoring the implementation of the findings from AML/ CFT & compliance risks reviews or regulatory inspections, providing guidance to the Business Units on corrective action to be taken for identified AML/ CFT CDD & compliance breaches/incidents, and tracking the breaches/incidents and their appropriate resolution.

The Compliance department shall identify compliance failures in the bank using the internal audit and concurrent audit as a feedback mechanism. Summary of all audit reports will be marked to Chief Compliance Officer. It will go through the summary of all audit/inspection reports and rectification reports regularly to enable it to identify compliance failures in the bank The Compliance department shall monitor and test compliance by performing sufficient and representative compliance testing and report the results thereof to the Senior management.

While performing duties Compliance Department shall have all the rights to have access to all kind of obtained information of clients and beneficiaries.

9. Policies and Procedures

The Bank shall have and effectively implement internal policies, procedures, systems, controls and customer acceptance policy that clearly indicates situations when a customer will be rejected.

This policy is intended to address the following:

i. Risk evaluation of the customer, products, services, geographic locations, and delivery channels as well as transactions;

ii. Identification and verification of the customer and beneficial owner including walk-in/occasional customers, and politically exposed person(s) ;

iii. Application of customer due diligence measures;

iv. Maintaining records and information obtained in the CDD process and information of transactions;

v. Monitoring of transactions, including monitoring to identify unusual or suspicious transactions;

vi. Reporting to FIU of threshold transactions;

vii. Reporting to FIU of suspicious transactions;

viii. Ensuring that internal policies, procedures, systems and controls are subject to independent testing and review;

ix. The appointment of a Chief Compliance Officer at Senior Management level to ensure compliance with the provisions of the AML/CFT law and the NBTs regulation thereon;

x. Ensuring high standards while recruiting employees. This shall include separate requirements for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing;

xi. Establishing training programs and providing on-going trainings to all new and existing employees, directors, board members, executive or supervisory management;

xii. Other arrangements as prescribed by the NBT.

The Bank shall ensure that all of its internal policies, procedures, systems and controls remain consistent with the risks and complexity of operations and are adopted by the bank's Board of Supervisors and shall be applicable to all domestic and foreign branches if any.

10. Customer Acceptance/ Rejection

10.1. 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 (10).

10.2. 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.

10.2. 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.

11. Risk Assessment

The Bank shall assess and understand its money laundering and terrorism financing risks, including of new products or technologies. The risk assessment and any underlying analysis and information shall be documented in written form and be kept updated and readily available for NBT to review at their request.

The Bank shall document the risk assessments in order to be able to demonstrate their basis, keep the assessments updated, and make the documents of the processes and the risk assessment documentations available to NBT upon request.

11.1. ML/TF Risk Assessment of the Business

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.

11.2. 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.

11.3. Risk Management

The ML/TF risk of each bank is specific and requires an adequate risk management approach, corresponding to the level and structure of the risk, and to the size of the bank. The objectives and principles of NBTs risk management should enable entities to establish a business strategy, risk appetite, adequate policies and procedures, promote high ethical and professional standards and prevent entities from being misused, intentionally or unintentionally, for criminal activities.

ML/TF risk management requires attention and participation of several business units with different competences and responsibilities. It is important for each business unit to precisely know its role, level of authority and responsibility within the bank's organizational structure and within the structure of ML/TF risk management.

11.3.1. Role of Management

Management gives direction to its business activities by setting the risk appetite, formulating objectives and making strategic choices from which subsequently policy and procedures are derived. Management should be able to determine the ML/TF risks of the business and take these into account in the bank's ultimate goals and strategies. Documentation and communication of strategy, policies and procedures are important for their actual implementation. Tools in this respect are, for instance, mission statements, business principles or strategic views. Management will also give direction to setting up, implementing and monitoring the NBTs control framework and will be responsible for the strategic choices to be made and decisions to be taken in that respect.

Management's leadership abilities in and commitment to the prevention of money laundering and terrorism financing are important aspects of implementing the risk-based approach. Management must encourage regulatory compliance and ensure that

employees abide by internal procedures, policies, practices and processes aimed at ML/TF risk mitigation and control. Management should also promote an ethical business culture and ethical behavior.

11.4. ML/TF Risk Monitoring and Review

Management should be able to adequately manage ML/TF risks, to verify the level of implementation and functioning of the ML/TF risk controls, and to ascertain that the risk management measures correspond to the bank's risk analysis. The bank should therefore establish an appropriate and continuing process for MLAF risk monitoring and review. This process will be done by the business control function to ensure on a regular basis that all processes are implemented; the compliance function to periodically monitor if the policies are adhered to and systems are in place; and the audit function to assess if the AML/CFT policies and process are conform the law and are performed in an adequate way.

Regular reports to management should contain the results of the monitoring process, findings of internal controls, reports of organizational units in charge of compliance and risk management, reports of internal auditing, reports of the person authorized for detecting, monitoring and reporting any suspicious transactions to FIU, as well as the findings contained in the supervisor's on-site examination reports on AML/CFT.

Management should be furnished with all important information which will enable it to verify the level of AML/CFT controls, as well as possible consequences for the banks' business if controls are not functioning properly.

The risk reports should indicate if appropriate control measures are established and adequate and fully implemented for the bank to protect itself from possible ML/TF misuse. The monitoring and review process should include the appraisal of ML/TF risk exposure for all customers, products and activities, and ensure the implementation of proper control systems, with a view to identifying and indicating problems before any negative consequences for the bank's business occur. This process may also alert the bank to any potential failures, for instance failure to include mandatory legislative components in the AML/CFT policies and procedures, insufficient or inappropriate customer due diligence, or level of risk awareness not aligned with potential exposure to ML/TF risks.

The bank must keep the ML/TF risk assessment up to date by setting up and describing the process of periodically reviewing the risk assessment. The bank must therefore also stay up-to-date with ML/TF methods and trends, international developments in the area of AML/CFT, and domestic legislation. Such a review can also include an assessment of the risk management resources such as funding and staff allocation and may also identify any future needs relevant to the nature, size and complexity of the bank's business.

Moreover, review should also be conducted when the business strategy or risk appetite of a bank changes or when deficiencies in the effectiveness are detected. When the

bank is to introduce a new product or activity, an ML/TF risk analysis of that product is to be conducted before offering that new product or services to existing or new customers.

12. High Risk Situations Requiring Enhanced Due Diligence

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

12.1. 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.

12.2. 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.

12.3. 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.

13. 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

13.1. 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.

13.2. 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.

13.3. 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.

14. 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.

14.1. 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.

14.2. Customer Identification Requirements

As per the Bank's policy the customer identification requirements shall include the following:

i. The Bank has already set up a system for the identification of the clients and to establish the identity of clients when performing any transaction for them;
ii. The Bank shall not maintain or open an anonymous account or an account in fictitious names;

iii. The Bank shall ensure to know the true identity of its customers including beneficial owners;

iv. Customer due diligence shall be carried out in the following cases:

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

b. Before carrying out domestic or international wire transfers.

c. Whenever doubts shall exist about the veracity or adequacy of previously obtained customer identification data

d. Whenever there is a suspicion of money laundering or terrorist financing.

14.3. 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.

14.4. 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.

15. Customer Screening Program

The bank shall use the following resources for screening customers:

a. UNSCs
b. OFAC (Office of Foreign Asset Control)

c. European Union

d. Office of Financial Sanctions Implementation (OFSI)

e. Internal lists provided by NBT

f. Banks own list of suspicious customers

The lists are being updated in internal program of the Bank (Oracle FlexCube) for the purpose of screening in 24 hours after update of the lists by authorized bodies.

Transactions of listed individuals and entities also transactions related to listed individuals or entities are subject to immediate stoppage and information related to such transaction being sent to FIU for assessment.

The bank freezes the assets of listed individuals and entities immediately without prior warning.

16. Politically Exposed Persons and risk Measure

The Bank shall establish appropriate risk management systems to determine whether a customer or beneficial owner is a politically exposed person (PEP) and if so, shall apply the following additional customer due diligence measures:

a. Obtain approval from senior management (CEO & in absence of CEO by other members of the management of the Bank) before establishing or continuing a business relationship with such a person or beneficial owner;

b. Take all reasonable measures to identify the source of wealth and funds of customers and beneficial owners identified as P EPs;

c. Apply enhanced ongoing monitoring to the business relationship.

16.1. Procedures for determining whether a customer or beneficial owner is PEP shall include:

i. Seeking relevant information from the customer or beneficial owner;

ii. Accessing and reviewing available information from any reliable source about the customer or beneficial owner;

iii. Accessing and reviewing commercial electronic databases of PEPs, if available.

17. 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.

18. 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.

19. 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.

20. Correspondent Banking Relationship

Before entering into a cross-border correspondent banking relationship or other similar relationships, in addition to performing normal customer due diligence measures the Bank shall:

i. Gather sufficient information about the respondent bank;

ii. Understand the nature of the respondent's business;

iii. Evaluate the reputation of the respondent institution and the quality of supervision to which it is subject, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

iv. Evaluate the anti-money laundering and combating the financing of terrorism controls implemented by the respondent bank;

v. Obtain approval from senior management before establishing new correspondent relationships. Clearly understand and document the respective anti-money laundering and combating the financing of terrorism responsibilities of each bank;

vi. Obtain copies of correspondent banks policies & procedures with regard to compliance;

vii. AML/CFT, customer acceptance, internal control measures etc.;

viii. Other measures considered necessary.

21. 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:

d. The full name of the originator;

e. 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;

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

g. 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;

h. 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.

22. Some Red Flags or Indicators of STR

Following are some of the indicators or red flags which may help compliance officers of Banks in Tajikistan to identify suspicious transaction and suspicious activities. The list of suspicious transaction and activities is provided by NBT (FIU):

i. Customer has an unusual or excessively nervous demeanor.

ii. Customer discusses your record-keeping or reporting duties with the apparent intention of avoiding them.

iii. Customer threatens an employee in an effort to discourage required record-keeping or reporting.

iv. Customer is reluctant to proceed with a transaction after being told it must be recorded.

v. Customer appears to have a hidden agenda or behaves abnormally,

vi. Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.

vii. Customer who is a student uncharacteristically transacts large sums of money.

viii. Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

ix. A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

x. Customer is unwilling to provide personal background information when opening an account.

After identifying suspicious transaction, the Bank sends STR to regulatory body.

23. Staff Safety

All the staff of the bank, employees, officers and related person's information and details; who conducts/conducted STR, SAR and related investigations & report against a money laundering or terrorist financing suspect shall be protected against disclosing their names and details to any third parties.

No criminal civil disciplinary or administrative proceedings for breach of banking or professional secrecy or contract shall lie against the Bank its directors, principals, officers, partners, professionals or employees who in good faith have submitted suspicious reports or provided information to FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

24. New products and business practices

Before launching new products, services and business practices or using new technologies the concerned department shall obtain sign off from Compliance department in the New products, Services and Technologies approval form by submitting all the relevant supporting documents for their review. The department shall identify, assess and take appropriate measures to manage and mitigate the money laundering or terrorism financing risks that may arise in relation to:

a. The development of new products, services and new business practices including new delivery mechanisms for products and services;

b. The use of new or developing technologies for both new and existing products.

25. Internal Policies, Procedures, Systems and Controls

The Chief Compliance Officer and other compliance staff shall have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The Chief Compliance Officer shall have the authority to act independently and to report directly to the Board of Supervisors.

The Board of Supervisors of the Bank shall periodically review the Bank's compliance with the requirements of the AML/CFT Law and the NBTs Regulation on AML/CTF. Such regular reports to the Board of Supervisors shall include a statement on all suspicious transactions detected, implications and measures taken by compliance staff to strengthen the financial institution's AML/CFT policies, procedures, systems and controls. Reports on suspicious transactions shall be general and not include any information on specific transactions or customers.

The Board of Supervisors shall also be informed of the results of any onsite inspections conducted by NBT, including remedial actions required to be implemented by the Bank.

The Bank shall maintain an adequately resourced and independent audit function to ensure that the Chief Compliance Officer and staff of the Bank are performing their duties in accordance with the bank's AML/CFT internal policies, procedures, systems and controls.

The Bank shall establish screening procedures when hiring employees. Such screening procedures shall include fit and proper requirements to be applied when hiring employees. More stringent fit and proper requirements are required for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing. Employee screening procedures and fit and proper requirements shall ensure that:

a. Employees have the high level of competence necessary for performing their duties as set out in their job descriptions;

b. Employees have appropriate ability and integrity to conduct the business activities of the bank;

c. Potential conflicts of interests are taken into account, including the financial background of the employee;

d. Fit and proper and code of conduct requirements are defined;

e. Persons convicted of offences involving fraud, dishonesty, money laundering or other similar offences are not employed by the bank.

The bank shall revise its policies once in a year or as when a material change occurs in the AML/CFT laws and regulations of Tajikistan or in the International arena. The policy will be drafted as per the regulations of NBT and relevant regulators; the same shall be put in forth for Board of Supervisors approval.

26. 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.

27. Staff Training

The Bank shall ensure adequate training to staff in the requirements of this policy and shall continually update the skills of the staff as per the requirements and change in situations. The training shall include real-world examples of transactions that constituted money laundering and terrorist financing, and an awareness of the role that staff play in the overall process of detecting and punishing money launderers and terrorist financers.

Compliance department shall provide adequate AML/ CFT & CDD trainings (such as AML/ CFT & CDD laws, regulations, policies, procedures, international best practices & standards) at least annually, to all relevant departments, branch managers, local and provincial branches, compliance officers at head office & branches, respected members of board of supervisors and, board of management

28. Anti-Bribery and Corruption measures

For the purpose of preventing bribery and corruption the Bank shall:

a. Limit the amount of gift can be received from customer (value of the gift should not exceed 50somoni).
b. Implement enhanced measures while performing transactions with government officials.
c. Implement other measures considered necessary.

Compliance department shall provide trainings related to anti-bribery and corruption as well as ethics related issues to the staff.

29. Final Provisions

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

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.

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

Reviewed & Recommended by Chief Compliance Officer for Approval.