ASIA ALLIANCE BANK

Anti-Money Laundering and Sanctions Compliance Program:

Know Your Customer (KYC) procedure

Tashkent – 2024

I. General rules

This Policy establishes and regulates the basic rules, principles and measures aimed at ensuring compliance of the activities of ASIA ALLIANCE BANK with combating the legalization of proceeds from criminal activity, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and sanctions, and also establishes the relevant functions and obligations of the divisions of ASIA ALLIANCE BANK.

The Bank is committed to complying with all applicable anti-money laundering and sanctions laws and regulations, including establishing banking relationships with customers (onboarding), opening new accounts, conducting one-off transactions and conducting regular audits.

2. The following key concepts are used in this Policy:

bank – JSCB "ASIA ALLIANCE BANK";

front office – employees, including senior employees of the bank's divisions, directly involved in customer service and responsible for customers' banking operations;

regulatory document – a bank's regulatory legal act (policy, regulation, procedure, instruction, etc.) that defines the main standards and approaches to the bank's activities in the following areas;

CDD – customer due diligence;

ML – money laundering;

rules – Internal control rules for combating money laundering, terrorism financing and the financing of the proliferation of weapons of mass destruction in commercial banks (registration of the Ministry of Justice of the Republic of Uzbekistan No. 2886 dated May 23, 2017);

risk appetite protocol – "ML/FT and sanctions risk appetite" protocol.

training program – a training program for the preparation and retraining of bank employees on AML/CFT and FPWMD issues;

Watch list – a list of individuals and legal entities provided by the SASB and associations for combating international economic crimes

ROBS – regional office of banking services;

SASB – specially authorized state body (Department for Combating Economic Crimes under the Prosecutor General's Office of the Republic of Uzbekistan);

Sanction – a coercive measure applied by states or international organizations to a state, legal entities and individuals who have violated international law;

FPWMD – financing the proliferation of weapons of mass destruction;

FT – terrorist financing;

Central Bank – the Central Bank of the Republic of Uzbekistan;

client – an individual or legal entity that carries out banking financial transactions;

bank account - an account opened by a bank for a client in accordance with an agreement under which the bank undertakes to accept and credit funds received on its account, to carry out the client's instructions to transfer and issue the corresponding funds and to carry out other operations on the account;

one off transaction - transactions carried out by clients on a one-time basis without opening a bank account, not repeated within one month;

escalation - notification of a higher level of the bank about questionable cases identified in the course of combating AML/CFT and FPWMD.

3. This Policy is mandatory for application in all divisions of the bank.

4. The Bank undertakes to comply with the legislation of the Republic of Uzbekistan, the Rules, sanctions, this Policy, as well as the following regulatory documents of the Bank:

Regulations on the Bank's Compliance Control Department;

Policy on combating the legalization of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction and compliance with sanctions;

Risk Assessment Procedure (RA);

Transaction Monitoring and Reporting Procedure (TM);

Sanctions Screening Procedure (SS).

5. The objectives of this Regulation are to ensure that the Bank has sufficient information about its clients and to verify the client’s identity for the following purposes:

Compliance with the legislation of the Republic of Uzbekistan;

Timely detection of abnormal/suspicious activity;

Minimization of the risk of the Bank being involved in illegal activities;

and Protection of the Bank’s reputation.

This Procedure implements the Bank's AML/CFT policy and includes the processes of identification and verification of the Bank's clients, customer due diligence, assessment of the risk rating of clients and enhanced due diligence. The set of measures defined in this order protects the Bank from activities related to money laundering, terrorist financing, proliferation of weapons of mass destruction and other financial crimes (collectively, AML/CFT), and ensures the risk-free nature and integrity of the Bank.

II. Responsibilities and Obligations

6. The Bank defines the following duties and responsibilities of employees within the framework of the Know Your Customer (“KYC”) Procedure:

6.1. Employees of the business line assume the following duties and responsibilities:

Conduct customer due diligence taking into account the risk level of customers;

Check the name of the customer and take appropriate measures based on the screening results;

Routinely check customers and make necessary changes;

When significant events occur, conduct event-based customer checks and make necessary adjustments accordingly.

6.2. Deputy Heads of the ROBS undertake the following duties and responsibilities:

Establish practical business relationships with low and medium risk clients and conduct periodic and event-based checks;

KYC, including collection of information and documents;

Escalation to Compliance Control Department staff in cases of significant risks.

6.3. The Head of the ROBS assumes the following duties and responsibilities:

Establish practical business relationships with high-risk clients and conduct periodic and event-based reviews;

Clarify measures to continue or terminate relationships with clients in agreement with the Compliance Control Department;

Escalate cases of serious risks to the Compliance Control Department and the Bank's management.

6.4. The Compliance Management staff undertakes the following duties and responsibilities:

Conduct periodic and event-based reviews;

Provide advice and guidance to staff on activities during the KYC process, as necessary;

Refer information to the Deputy Head of Compliance Management in the event that the screening of a client’s name reveals that the client is on a list or under sanctions;

In the event that manual changes to the risk level of clients are required, forward the relevant information to the Deputy Head of Compliance Management for formalization and verification;

Perform quality control checks on the KYC files of clients.

6.5. The Deputy Head of Compliance Control shall have the following duties and responsibilities:

When necessary, review cases of escalation by the employees of the Compliance Control Department;

Approve the establishment of practical business relationships with individual high-risk clients;

Check and monitor updated files in the screening database;

Fulfill the duties of the Head of Compliance Control in the event of his/her temporary absence for certain reasons.

6.6. The Head of Compliance Control shall have the following duties and responsibilities:

Confirm the need for manual change of the risk level of clients;

Update the compliance with the Bank List in the screening database updated by the Deputy Head of Compliance;

Approve the establishment of practical business relationships with individual high-risk clients;

For certain types of high-risk clients, perform quality control checks on KYC files;

Submit proposals to the Board of Directors of the Bank on the issues raised to further improve the efficiency of the KYC process;

Conduct periodic and event-based reviews;

In agreement with the Chairman of the Board, clarification of measures to continue or terminate relationships with clients;

If there are a large number of material risks, escalate them to the Chairman of the Board.

6.7. The Chairman of the Management Board assumes the following duties and responsibilities:

approval of the establishment of practical working relationships with local and foreign politically exposed persons (PEPs);

approval of conclusions of representative relationships with foreign banks;

if there are a large number of material risks, escalation of them for consideration by the Bank's Supervisory Board.

6.8. The Bank's Supervisory Board assumes the following duties and responsibilities:

approval of the establishment of practical working relationships with international politically exposed persons (PEPs);

consideration of issues raised by the Head of Compliance Control to further improve the effectiveness of the KYC process;

consideration of issues escalated by the Chairman of the Management Board and taking appropriate measures.

6.9. The Bank, including employees of the Compliance Control Department, managers and employees of other departments, shall be liable for violation of this Procedure in accordance with the law.

The Bank shall ensure that its payment agents and payment subagents comply with the requirements of this Procedure.

The Bank shall be liable for violation of the requirements of this Procedure by its payment agents and payment subagents.

In the event that evidence of violations of the law, as well as the legislation in the field of AML/CFT and FPWMD by Bank employees during transactions becomes known, Bank employees will immediately transfer this evidence in writing to the head or employees of the Compliance Control Department.

III. Prohibited Activities and Clients

7. Based on this procedure, the Bank prohibits the following activities and practical business relationships with clients that exceed the Bank's risk tolerance limit in relation to AML/CFT and sanctions, and terminates these activities and practical business relationships with clients identified during the inspection. It also prohibits one-off transactions.

8. The Bank prohibits the following activities:

8.1. Military industry - the Bank prohibits any activity related to the military business (financing, provision of banking services, investments and funds aimed at the military business).

8.2. Nuclear energy - the Bank restricts all activities related to the nuclear energy sector (financing, consulting or other banking services, investment funds focused on nuclear energy);

The Bank applies this restriction approach to the following entities and their respective suppliers:

Nuclear power plants (NPPs);

Nuclear fuel mining, processing and trading companies;

Nuclear waste management companies (storage of spent fuel from nuclear power plants).

8.3. Gambling - The Bank restricts all activities related to gambling, casinos and other games based on risks.

In particular, this activity is prohibited by law in the territory of the Republic of Uzbekistan. It also does not provide banking services to clients engaged in this type of activity.

8.4. Sexual exploitation - The Bank prohibits any activity based on sexual exploitation.

9. The Bank prohibits entering into practical business relationships with the clients listed below. It also terminates business relationships with the following types of clients identified during ongoing inspections:

9.1. Shell banks are financial institutions that do not have a physical presence in any country or do not have permanent financial regulators;

9.2. Correspondent banks providing products and services to shell banks;

9.2.1. Shell organizations;

9.3. Unlicensed financial institutions;

9.4. Licensed money service providers (MSB);

9.5. Licensed money transfer service providers (PSP);

9.6. Providers that convert funds from one currency to another

9.7. Providers of unlicensed virtual (cryptocurrency) asset transfers, e-wallets and risk-based gambling.

9.8. Unregistered virtual (cryptocurrency) asset service providers in the Republic of Uzbekistan;

9.9. Natural or legal persons known or seriously suspected of involvement in money laundering or terrorist financing;

9.10. Clients refusing to provide information as required by law:

clients providing false or inappropriate information;

high-risk clients whose identification information has not been verified.

9.11. Opening or operating anonymous accounts or accounts under a fictitious name;

9.12. Charitable, non-profit and non-governmental organizations established in high-risk countries.

9.13. Sanctioned parties that do not have a permit or license include: individuals, legal entities or organizations included in the List provided by a specially authorized government agency;

individuals, legal entities and organizations established in a country or territory where they are considered residents of this territory to which comprehensive sanctions apply;

foreign representative offices of banks.

9.14. Entering into business relationships with high-risk clients without their personal involvement;

9.15. Establishing and maintaining relations with non-resident banks not located in the territory of their countries of registration, and their permanent management bodies;

9.16. Establishing subsidiary banks, branches or representative offices in the territory of countries not participating in international cooperation in the field of combating money laundering and terrorist financing;

9.17. Persons residing, located or registered in a country that poses a threat to the international financial system according to the official statement of the Financial Action Task Force (FATF);

9.18. In other cases determined by the Compliance Control Department.

IV. Clients subject to KYC procedure

10. The Bank applies appropriate KYC measures before conducting transactions with clients in the following cases:

10.1. New clients: In the process of establishing practical business relations with the bank;

When an individual applies for credit services;

When an individual applies for a bank card;

When applying for services for storing valuables in bank deposit boxes;

When legal entities and/or individuals own shares of commercial banks in an amount equal to or exceeding one percent of the authorized capital;

When applying for the purchase of securities issued by a commercial bank.

10.2. A current client who continues to operate:

When applying for a bank loan.

10.3. A previous client with whom practical business relations have ended:

In the process of restoring business relations or when applying for a bank loan.

10.4. Exceeding a certain limit amount, conducting one or more suspicious transactions, as well as clients performing one-off transactions specified in paragraph 14. of this procedure;

10.5. In case of suspicion that the client or his transactions are related to ML/FT;

10.6. In case of doubts about the sufficiency of previously received information for the purposes of identification or verification of the client's identity;

10.7. In other cases requiring identification of the client.

A) New clients

11. Front office employees apply KYC measures before establishing a practical business relationship with a client or when applying for the use of bank credit services. However, if it turns out that the client belongs to the high-risk category, the Bank applies enhanced due diligence (EDD) measures. A scanned copy of all provided information and documents related to the KYC process must be displayed in his questionnaire.

B) Existing client who continues to operate

12. Employees of business areas apply KYC measures to an existing active client when opening a new account or when applying for the use of bank credit services.

Dormant or inactive accounts mean clients who, as determined by the Bank, have been inactive for more than 9 months. The measures specified in paragraph 11 of this procedure shall be applied to such dormant or inactive clients.

C) Previous Client with whom the practical business relationship has ended

13. In cases where the business relationship has already been terminated, but an application has been submitted for opening a new account with the Bank, all necessary KYC measures must be carried out for the new potential client.

Client details from an existing previous file cannot be used to complete the client's KYC file. Also, the Business Line staff should first consider the rationale for terminating the previous relationship with the client. When conducting an investigation, the Business Line staff, if necessary, in consultation with the Compliance Control Department, should consider the reasons for the previous termination, including: **reasons for filing the ODR;**

in accordance with the red flags identified, the level of severity, or the specific situation of the client;

material negative news;

unusual or suspicious activity; law enforcement actions or investigations.

D) One-off transactions

14. KYC measures are implemented in the following cases, when the execution of one-off transactions, including the execution of one or more linked transactions, exceed a certain limit amount:

14.1. In case of withdrawal of foreign currency in cash by clients from the bank's cash desks through bank cards issued by another bank, in an amount equal to or exceeding 100 times the BCV;

14.2. When individuals purchase foreign currency in an amount equivalent to more than 100 US dollars;

14.3. In the process of carrying out all transactions without opening a bank account or using an account in an amount equal to or exceeding 500 times the BCV;

14.4. KYC measures are also implemented for senders of domestic P2P electronic money transfers, which are received in the accounts of the bank's clients in an amount equal to or exceeding 34 times the BCV.

15. Information obtained as a result of the necessary verification of customers who have made one-off transactions will be updated during subsequent transactions for which KYC measures are required.

D) Customers acquired through mergers or acquisitions

16. In case of a merger (with other banks or branches of the bank) or acquisition of the Bank, the Bank will apply a risk-based approach to reviewing newly accepted customers and accounts.

17. In case of a merger or acquisition, the Bank will immediately check the profiles of acquired customers in accordance with its customer risk assessment methodology.

Accepted customers, including high-risk customer profiles, shall be checked immediately. Medium and low-risk customer profiles shall be checked as soon as possible in accordance with established practice.

18. The Bank will develop an action plan to improve customer and account profiles added to the standards mentioned in the KYC procedure.

V. Identification and verification of clients

19. Identification and verification of clients are carried out after the Bank has established the true identity of its clients, individuals acting on their behalf, and/or individuals or legal entities exercising control over the client.

After the identification of clients, their data is stored in the KYC form. For individuals ("Individual KYC form" See Appendix A). For individual entrepreneurs (see Appendix B "KYC form for individual entrepreneurs"). And for legal entities (see Appendix C "KYC form for legal entities").

20. When legal entities and individual entrepreneurs, whose founders are residents of the Republic of Uzbekistan, apply for opening a bank account remotely or through an application from the Bank during the state registration process, customer verification measures can be carried out by State Service Centers or sent through the online banking platform, and commercial banks can trust the results of the measures taken.

21. In case of doubts about the reliability of the information received during the previous procedure of identification of the client and (or) the beneficiary of the property, the Bank will repeat the identification procedure in the established manner.

A) Minimum requirements for identification

The following minimum identification information must be obtained from individuals and legal entities, as well as individual entrepreneurs and verified by appropriate verification methods before entering into practical business relations with the client or opening an account.

Regardless of whether it is a legal entity or an individual, all documents submitted confirming the identity of the client must be valid on the date of submission to the Bank.

23. Information required to identify individuals:

last name, first name and patronymic (in Latin);

date and place of birth;

citizenship;

permanent and (or) temporary place of residence;

identity card; (Passport, ID card or other document replacing them)

personal identification number of an individual (PINOI);

telephone number.

24. Information required to identify individual entrepreneurs:

information required in paragraph 23 of this procedure;

information on state registration: date, number, name of the registering authority; place where the activity is carried out;

other information specified in the certificate of state registration;

information on current certificates and licenses for the activity:

type of activity, license number, date of issue;

by whom it was issued;

expiration date;

telephone numbers.

25. Information required for identification of legal entities:

full and abbreviated name, if indicated in the state registration certificate;

state registration information: date, number, name of the registering authority; taxpayer identification number;

location (postal address), as well as the address of the location and the address of the head office, if different from the first;

other information specified in the state registration certificate;

information on the availability of licenses for licensed types of activities:

type of activity, license number and date of issue; by whom it was issued;

expiration date;

information on the identification of individuals with the right to sign, or an individual acting on behalf of the legal entity;

information on the founders (major shareholders, participants) of the legal entity and their shares in the authorized capital (capital) of the client;

information on the amount of the registered and paid authorized capital (capital);

information on the full identification of the client's beneficial owner.

information on the governing bodies of the legal entity (structure and personnel of the governing bodies of the legal entity);

telephone numbers.

B) Identification and verification check methods

26. The introductory part of the KYC identification and verification process consists of collecting information related to the identification information received from the client. This process should be performed until all information, including the identification information of the client, is verified. If it is not possible to conduct a proper investigation of the client, any practical business relationship with such client should be terminated.

27. Front office staff should reflect the identification information provided by the client and implement procedures, including applicable risk-based approaches, to verify the identity of each client. The reception, storage and verification of information and documents on clients is assigned to the employees of the business line.

C) Identification and verification by documented and undocumented methods.

28. Employees of the activity area are responsible for collecting identification information about the client and verifying it using documented and undocumented methods.

Documented methods for verifying information received from the client are carried out for legal entities, individual entrepreneurs and individuals by checking the originals of the documents they provide.

29. For individual residents with a low and medium risk level, the Bank can accept and verify the identification data they provide remotely (online) or through the Bank's application.

30. Legal entities and individual entrepreneurs whose founders are residents of the Republic of Uzbekistan can apply for opening a bank account remotely (online) or through the Bank's application during the state registration process. In this case, front office employees enter into practical business relations after verifying the client by generating a KYC form for the identification data of the legal entity.

31. It is prohibited to open an account remotely (online) and enter into practical business relationships with clients belonging to the high-risk category.

D) Sending notifications to clients

32. Front office staff must send a notification to confirm the identification data provided by clients remotely (online) and to verify them.

The notification (consisting of four or five digits) will be sent to the phone number or email address specified by the client.

After entering this notification into the banking application, its verification is confirmed.

E) Failure of the verification process

If the verification process cannot be carried out, including in cases where the Bank acts through its payment agents and/or subagents, the Bank considers the KYC process incomplete and with such clients:

refuses to establish business relations with new clients;

refuses to carry out any transactions;

it will be necessary to take measures to terminate the current working relations.

VI. Customer Due Diligence (CDD)

34. CDD data of customers who attract new customers, open new accounts or carry out one-off transactions exceeding the established identification limit shall be collected by line of business personnel.

34.1. Line of business personnel shall ensure that the information provided in the customer questionnaire matches the customer’s identification documents (passport, ID card, etc.) and the results are documented in the customer’s KYC file.

34.2. The information collected shall be used by the Bank to form an initial understanding of the customer’s expected profile and activities, as well as to determine the customer’s risk of money laundering that the Bank may face.

34.3. Changes to the CDD data shall be made by the relevant line of business personnel.

Line of business personnel shall store new or updated CDD information in the KYC file along with the relevant documents.

The CDD measures implemented by the bank include: identification and verification of the client;

identification of the person acting on behalf of the client, verification of identity and authority; determining the beneficial owner of the client;

studying the type of activity, purpose and nature of the planned transactions;

continuously monitoring the business relationships and transactions carried out by the client, checking their compliance with the information and business activity of the client, the risk profile, including, where necessary, compliance with the sources of funds.

A) Individual Due Diligence

35. In accordance with the Bank's policy, the CDD process is carried out for all individual customers, including individuals and legal entities acting on behalf of such customers.

36. Customer Identification Information As part of the CDD process, the following additional information must be collected and maintained about each individual customer and any person acting on behalf of such customer: occupation;

job title;

transaction purpose;

expected number of transactions;

37. Front office employees are responsible for the following when verifying documents received from an individual (customer) wishing to open an account with the Bank or from reliable sources:

verifying the accuracy of all documents;

verifying the information provided by documented and undocumented methods;

requesting any additional documents necessary to satisfy the requirements established by this Procedure.

38. Primary identity documents and secondary identity documents, where applicable, are required to verify the identity of an individual customer. Any supporting documents provided by the customer and retained for CDD purposes must be reviewed with the original documents and copied.

38.1. An identity document is considered a valid government-issued identity document that can be used to verify the identity of a client who is an individual.

The following are the identity documents accepted by the bank:

Passport of the Republic of Uzbekistan;

Passport of the Republic of Uzbekistan for travel abroad;

ID card of the Republic of Uzbekistan; Driver's license of the Republic of Uzbekistan;

Military ID of the Republic of Uzbekistan;

UN resident passport;

(red or blue) passport of citizens of the Republic of Uzbekistan who have not reached the age of majority;

Death certificate;

Passport of a foreign citizen;

Certificate of residence in the Republic of Uzbekistan for a foreign citizen (ID card);

Residence certificate (ID card) for stateless persons;

Birth certificate.

39. In addition to documentary verification methods, the employees of the line of business are responsible for using undocumented methods to verify the identification data of the individual client. The following are examples of undocumented methods of confirming the identity of an individual client: documenting in the client's KYC file whether the photo provided remotely (online) matches the person's appearance;

(Determining as a result of a face-to-face meeting between the employees of the line of business and the client who is an individual);

by online verification using new technologies through the Bank's mobile application (sending a photo or video file of the client's face);

checking the compatibility of the information provided by the individual client and the information in the current identity document issued by the state;

calling the client to check the provided means of telephone communication.

39.1. The employees of the activity area are responsible for independently verifying the identity of the client by comparing the information provided by the individual client with the information obtained from the above sources.

B) Legal Entity Due Diligence

40. According to the Compliance Policy, the CDD process is carried out in relation to all clients that are legal entities, including individuals or legal entities acting on behalf of the client (trusts, authorized representatives, external management), as well as foreign legal entities that do not have legal management.

40.1. The client identification procedure is carried out in relation to the legal entity, the person controlling the legal entity, the beneficial owner, individuals acting on behalf of the legal entity (for example, persons with the right of signature) and, if it is considered necessary, parties to the transactions of the legal entity. This section sets out the mandatory requirements for the CDD process, which is mandatory for all clients related to an individual who is a legal entity, before the completion of the transaction.

41. In order to establish practical business relationships with legal entities, front office employees must collect and store the following additional information:

type of client;

scope of activity; purpose of the organization (for a non-profit organization);

country in which the legal entity is established (for permanent establishments and representative offices);

country(ies) where the activity is carried out;

purpose of the transaction; number of expected transactions;

level of assets;

B1) Methods of verification of a legal entity client

42. When checking documents received from a legal entity wishing to open an account with the bank or through reliable sources, employees of the activity area are responsible for the following:

checking the correctness of all documents;

checking the provided information using documented and undocumented methods;

requesting all additional documents necessary to meet the requirements established by this Procedure.

B2) Documented methods used in verifying a legal entity

43. Front office employees must familiarize themselves with the original documents submitted by the legal entity and make copies of them.

43.1 The main documents confirming the identity of a legal entity include:

memorandum of association of a legal entity;

certificate of state registration;

license issued by authorized organizations;

Taxpayer identification number;

Accreditation certificate etc.

B3) Undocumented methods used to verify a legal entity

44. Front office employees are responsible for using undocumented methods to verify identification data obtained remotely (online) or through the Bank application of a legal entity whose founders are residents of the Republic of Uzbekistan.

44.1. Examples of undocumented methods for confirming the identity of a legal entity:

verification of compliance of information provided by a legal entity (beneficiary, controlling party and person authorized to sign) and the actual identification information provided by the state;

verification of contact information received by telephone from a legal entity;

independent third-party sources (e.g., Public Service Centers, including but not limited to www.register.stat.uz www.fo.birdarcha.uz www.openinfo.uz) to verify the correctness of supporting documents received from a legal entity client, to verify the compatibility of information;

if necessary, study the place of business (mailing address) of the legal entity (i.e., physical visit);

study the official website of the legal entity, if any.

44.2. Front office employees are responsible for reviewing the relevant information and clarifying the following issues: the presence or absence of a legal entity;

whether the legal entity is registered to carry out business activities at the place of its incorporation on legal grounds;

studying documents certifying the relevant powers of the representative acting on behalf of the legal entity.

Accounts are opened for clients after verification of the identification data that the client sent remotely (online) or through the Bank's application. Limits can be set according to the principle of the Bank's Risk-Based Approach procedure for clients who opened an account through the Bank's application (online).

It is prohibited to open an account in foreign currency through the Bank's application.

C) Identification and verification of related parties

C1) Beneficial Owner

In addition to conducting the required due diligence on customers, the Bank should take additional steps to determine the details of the beneficial owners of customers during the KYC process.

In the course of applying CDD measures to a legal entity, the Bank is required to identify and verify the identity of the customer and examine the nature of its activities, as well as the ownership or management structure. In particular, the front office staff shall determine the beneficial owner of the customer and take appropriate steps to verify the identity of such persons in accordance with the following conditions:

I. Identification of the natural persons who, if any, directly or indirectly through any contract, agreement, transaction, relationship or otherwise own 10% or more of the equity interest in the customer that is a legal entity ("Ownership Prong");

II. If there is doubt as to whether the individual(s) with a controlling interest are the beneficial owner(s) referred to in paragraph (I), or if no individual has control through an ownership interest, then the individual of one person, i.e. the person who holds controlling control or significant liability of the undertaking, shall be recognised as the beneficial owner (the "Control Prong");

III. In the event that it is not possible to identify the individual in accordance with (I) or (II) above, the Bank shall identify the relevant individual holding the position of senior official and take appropriate steps to verify his or her identity.

46.1. The Bank obtains beneficial ownership information from the beneficial ownership certification form for legal entity customers (see Appendix D, “Certificate of Beneficial Ownership”) and other relevant information provided to the Bank during the required due diligence. This certification form can also be completed electronically.

47. Individuals shall also undergo identification and verification of the beneficial owner by the Bank if deemed necessary. In the event that an individual is suspected of having a person other than himself who ultimately manages or controls him, the Bank shall conduct a process of re-identification and verification of the beneficial owner.

48. The process of identifying the client-beneficiary-owner shall be carried out on the basis of the requirements of paragraph 23 of this Procedure.

49. When it is established that the real owner of a legal entity is another enterprise or organization, the method of determining the real owner of such enterprise or organization shall be carried out on the basis of paragraph 46 of this Procedure.

50. The period of documents required for verification of the beneficial owner shall not exceed six weeks.

51. If the client or the beneficial owner of the client is a legal entity that is subject to the following regulatory requirements on the disclosure of information on the ownership structure, identification and verification of the founders of such legal entity (shareholders, participants owning at least ten percent of the shares of the company) is not required:

government;

financial institutions regulated by the relevant regulatory authority in each country;

legal entities whose ordinary shares or shares are publicly traded on a recognized stock exchange (other than financial institutions);

a legal entity that is subject to a regulatory requirement to disclose information on the ownership structure.

51.1. The beneficial ownership exemption also does not apply to:

senior officials or licensed sanctioned clients;

clients associated with senior officials or licensed sanctioned persons.

51.2. In order to improve the efficiency of the internal control system in banks and to comply with international requirements, the Central Bank, based on the "Recommended Guidelines for Determining the Beneficial Owner of a Client for Banks, Non-Bank Credit Institutions and Payment Institutions" , determines the beneficial owner of a Bank's client and introduces guidelines on the identification methodology. For more details, see the "Methodology for Determining the Beneficial Owner of a Client in Appendix I" of these Regulations.

D) Person authorized to sign

52. A person authorized to sign is an individual appointed by the client to perform transactions on behalf of the client. This person may or may not own funds in the account or be the holder of a controlling stake in the client. If it is established that an authorized signatory holds several positions (for example, an authorized signatory or a beneficial owner), the necessary information related to each position must be documented.

52.1. Documents confirming that the designated signatory is authorized to act in that capacity must be obtained and stored in the client's KYC file.

53. The following information is required from signs: identification information for individuals.

D) Confirmation of required customer verification

54. Responsible persons shall review all documents received from customers and approve and complete the KYC procedure for customers as follows:

54.1. For individuals:

For low-risk customers – Head of Business Line;

For medium-risk customers – Deputy Head of Operations Department (ROBS);

For high-risk customers – Head of Operations Department (ROBS), in certain cases – Head of Compliance Control Department or his/her deputy.

54.2. Legal entity and sole proprietor:

For low-risk customers – Head of Business Line;

For medium-risk customers – Deputy Head of Operations Department (ROBS);

For high-risk customers[1] – Head of Operations Department (ROBS), in certain cases Head of Compliance Control Department or his/her deputy.

55. Establishment of banking business relations with clients with certain types of high-risk transactions, with the possibility of performing high-risk transactions, is carried out after approval of the Compliance Control Department.

56. In the event of disagreement between the front office and the Compliance Control Department on issues of establishing practical business relations with a client, the situation will be escalated to the Bank's Management. Any decision to establish or refuse to establish practical business relations with clients, taken by the Bank's Management in accordance with this section, is final.

VII. Client Screening

57. The client screening process, as part of the KYC procedure, is required for all individuals and entities upon initiation of practical business relationships and periodic reviews.

This requirement includes:

- Clients (individuals/entities);
- Beneficial owners;
- Other related parties, including authorised signatories or traders, power of attorney holders, attorneys-in-fact, representatives, executors and guarantors (if applicable).

[1] In certain cases – paragraph 81. of this procedure - (Process for approving verification of high-risk clients) The Head of the Compliance Control Department or his deputy is provided with complete information on what type of clients needs to be approved.

58. Client name verification must be performed prior to account opening and during the ongoing verification process. Line of Business staff are responsible for the initial verification of client names during client account opening and the ongoing verification process. Alerts generated must be forwarded to the Compliance Management staff for further investigation and resolution.

A) Watch List Filtering System

59. The Watch List System includes the following lists used by the Bank to determine whether a customer and persons associated with the customer are designated:

Common List of Terrorist Designated Persons (CTS) issued by the United Nations (UN);

Consolidated Sanctions List issued by the United States of America (OFAC);

Sanctions List issued by the European Union; Sanctions List issued by the United Kingdom; Politically Exposed Persons List;

Persons (including individuals, undertakings and organisations) whose nationality or place of residence is one of the countries with strategic weaknesses as defined by the FATF;

List of Persons Involved or Suspected of Involvement in Terrorist Activity or Proliferation of Weapons of Mass Destruction issued by the SASB**;**

A1) Alert Review Procedure

60. As part of the customer identification and verification process, the bank shall check the names of customers against the Watch List system. In addition, all customers and their beneficial owners, signatories, transaction participants and "Payment Details" shall be checked against the Sanctions Screening List.

61. Front office staff will conduct an initial review of the identified alert If the customer identification information in this alert matches a person in the Watch List system in full, partially, unclearly or incorrectly, it will be forwarded to the Deputy Head of Compliance Control or the Compliance Control staff

Watch List System Filtering Process

The bank's line of business staff shall determine whether the customer's name matches any persons in the Watch List system during the real-time KYC process, including during the process of entering into a practical business relationship with the customer or opening an account. This process may also be performed automatically. In the event of any changes to the Watch List system, Compliance Control staff must perform a "mass verification process" of filtering.

A3) Watchlist System Management

63. The Deputy Head of Compliance Control Department monitors, manages and ensures the Watchlist System database updates.

A4) World Check, Sanction Screyening Utility

64. This system is used by the Bank to determine whether a client is subject to sanctions, AML/CFT, whether the client or its beneficial owner is a senior official and in other cases. It is also used in relation to the client's counterparty, clients for one-off transactions, checking negative news. In these systems, the database update process is performed automatically.

A5) National Monitoring System

65. This system, based on the List provided by the Department for Combating Economic Crimes under the Prosecutor General's Office of the Republic of Uzbekistan, checks the Bank's clients, their beneficial owners, clients' counterparties, clients' transactions ("Payment Content") and other cases in relation to persons included in the List.

65.1. Control over whether the list is updated on the official website of a specially authorized government agency or monitoring of receipt via an electronic communication channel is carried out by the branch for work with requests and sanctions lists of the Compliance Control Department.

65.2. The branch shall provide access to relevant employees, including employees working directly with clients, by entering the List into the Bank’s automated system within three hours from the moment the List is posted on the official website of the specially authorized government agency or received through electronic communication channels.

B) Negative News

66. All customers and their beneficial owners should be screened for negative news prior to entering into a practical business relationship or during periodic and event-related reviews. After screening, each result is marked as “compliant” or “non-compliant”.

67. Negative news is divided into “compliant” and “non-compliant”. If there is any doubt about the compliance of a negative news item, front office staff should seek clarification from the Compliance Control Department staff.

67.1. Relevant Negative News Terrorist activity related to FT and FPWMD;
AML and sanctions non-compliance;
Drug-related crimes;
AML-related fraud;
AML-related bribery;
Individuals blacklisted or watchlisted by government due to increased AML risk;
law enforcement investigative decisions (e.g. indictment, arrest, forgery, etc.);
criminal charges or convictions (e.g. indictment, arrest, forgery, etc.);
significant civil damages or fines due to increased AML risk;
being subject to AML-related fines;
corrupt activity;
existence of an AML risk in the content of defamatory articles.

67.2. Irrelevant Negative News Convictions or criminal records;
imposed civil fines;
employee misconduct;
conduct of former senior management;
minor disputes with third parties;
minor operational deficiencies; network routine disturbances;
client appointed to a high political position;
personal matters unrelated to the client’s activities or those of its affiliates.

68. In cases where Front Office staff do not have reasonable assurance about the "match" and "non-match" of cases in the above sample category, they will consult with a member of the Compliance Management Department.

69. To address the risk of an unspecified client balance, Front Office staff may search publicly available domains. The results of a negative news search may prevent potential risks that the client may pose to the Bank, such as disclosure of information about regulatory actions, ongoing investigations, or allegations of financial crimes or other serious violations.

70. As part of the due diligence process, front office staff will search public domains (Google, Yandex, etc.) prior to entering into practical business relationships with clients and their beneficial owners or during periodic and case-based due diligence.

71. In the process of searching public domains, line of business staff will search for the full name of the client using the following search strings:

"**Client name**" and "abuse" or "allegation" or "arrest" or "blackmail" or "breach" or "bribery" or "convicted" or "corruption" or "criminal" or "drug" or "embezzle" or " evasion" or "extremist" or "fined" or "forge" or "fraud" or "guilty" or "illegal" or "money laundering" or "politically exposed" or "prison" or "prosecution" or "sanctions" or "scam" or "scandal" or "stolen" or "suspect" or "terrorist" or "theft" or "trafficking".

"**Customer name**" and "abuse" or "charge" or "arrest" or "blackmail" or "violation" or "bribery" or "convict" or "corruption" or "criminal" or "drugs" or "embezzlement" or "evasion" or "extremist" or "fined" or "counterfeit" or "economic crime" or "guilty" or "illegal" or "money laundering" or "politically exposed" or "prison" or "charge" or "sanction" or "fraud" or "scandal" or "stolen" or "suspect" or "terrorist" or "theft" or "illegal trade".

72. The Activity Line staff will review at least the first two pages of search results for the last five years. If the search results return less than two pages, the Activity Line staff will review all information. Additional searches, such as name changes, may be conducted based on the professional judgment of the Activity Line staff. Further guidance on this matter can be found in this Policy. (See **Appendix E**, *Public Domain Search Methodology*).

VIII. Client Risk Level

73. The Bank assesses the potential risks for each client using information obtained in the process of entering into practical business relationships with clients, opening a new account, periodically reviewing or making changes to the KYC file of an existing client.

73.1. The Bank divides clients into three categories according to their risk level:

High;

Medium;

Low.

74. The following criteria apply to high-risk clients:

a) Persons or organizations included in the list, owned or controlled by a person included in the list, Direct or indirect owners or controlling persons of organizations included in the list;

b) Persons permanently residing, located or registered in countries that are considered to have strategic deficiencies in the fight against money laundering and the financing of terrorism;

c) representative offices of foreign enterprises and individuals who are non-residents of the Republic of Uzbekistan; d) persons permanently residing, located or registered in an offshore territory;

e) residents and non-residents who have accounts in offshore zones;

f) organizations and individual entrepreneurs whose actual location does not correspond to the information specified in the constituent or registration documents;

g) organizations whose beneficial owners are the persons specified in subparagraphs "a)" and "b)" of this paragraph;

h) clients who regularly (e.g. for 3 months in a row) carry out dubious or suspicious transactions;

i) clients using software packages that do not have the ability to properly verify the client;

j) politically exposed persons (PEPs), their close relatives and persons close to politically exposed persons;

k) a foreign structure that is not a legal entity;

l) persons to whose accounts 20 or more bank cards are linked;

m) organizations whose beneficial owners are persons specified in subparagraph "d)" of this paragraph;

n) international charitable, non-profit and non-governmental organizations;

o) entrepreneurs engaged in jewelry, precious metals, works of art and antiques;

p) High-risk clients, who are assessed in the KYC process based on the risk arising from banking products, channels, profession, position and volume of transactions;

q) clients belonging to the high-risk category in terms of sanctions;

r) clients who do not meet the above criteria, but who have been found to have doubts regarding AML/CFT and FPWMD (e.g.: Crypto assets, P2P and others);

s) organizations whose beneficial owners are persons specified in subparagraph "j" of this paragraph;

t) clients associated with negative news or negative media.

75. Clients falling into the medium-risk category consist of the following criteria:

a) organizations and individual entrepreneurs whose period of activity does not exceed one quarter of the financial year;

b) Clients with a medium risk level, who are assessed based on the risk arising in the KYC process, based on banking products, channels, profession, position and volume of transactions;

c) Foreign citizens who are residents of the Republic of Uzbekistan;

d) clients whose founders or beneficial owners are not citizens of the Republic of Uzbekistan; e) clients who do not meet the above criteria, but who have suspicions regarding AML/CFT and PF;

f) Temporarily unemployed person who is a citizen of the Republic of Uzbekistan.

76. All clients who do not meet the requirements of paragraphs 74 and 75 of this procedure are classified as low-risk clients.

77. As part of the risk-based approach, the Bank examines various risk factors associated with each client: during the establishment of a practical business relationship with the client; during periodic and/or incident-based verification.

IX. Enhanced Due Diligence (EDD)

78. When classifying a customer or a transaction carried out by a customer as high risk, commercial banks shall apply the following enhanced due diligence measures in relation to such customer:

I. Front office employees:

collect additional verified information about the customer from open sources and databases and include it in the electronic KYC file or provide it to the Compliance Control Department employees;

obtain information from the customer on the sources of funds or other assets in connection with the transactions carried out by him and include it in the electronic KYC file or provide it to the Compliance Control Department employees;

II. Compliance Control Department employees:

examine the information entered or provided in the KYC file by the front office employees;

examine the purposes and nature of the transactions planned or carried out by this customer; establish ongoing monitoring of the transactions carried out by this customer;

obtain other additional information for the implementation of internal control.

79. If it is not possible to apply enhanced measures to conduct due diligence on a client, in particular, to obtain information from the client about the sources of funds or other assets for the transactions carried out by the client and (or) to study the purposes of the transactions planned or carried out by the client, the bank refuses to carry out the transactions of such client.

80. Information about the sources of funds or other assets for the transactions carried out by the client is stored electronically in the client's KYC file or is stored in special files of the Compliance Control Department.

High-Risk Client Due Diligence Approval Process

The Head of the Compliance Control Department or his/her deputy, in the process of establishing practical business relationships with a client or conducting periodic audits, participates in the process of approving clients classified as falling into the following high-risk category specified in paragraph 74 of this Procedure:

a) Persons or organizations included in the list, owned or controlled by a person included in the list, Direct or indirect owners or controlling persons of organizations included in the list;

b) Persons permanently residing, located or registered in countries that are considered to have strategic deficiencies in the fight against money laundering and terrorist financing;

d) Persons permanently residing, located or registered in an offshore territory;

g) Organizations whose beneficial owners are the persons specified in paragraphs "a)" and "b)" of this paragraph;

j) Politically Exposed Persons (PEPs), their close relatives and persons close to politically exposed persons;

m) Entities whose beneficial owners are persons specified in subparagraph "d)" of this paragraph;

r) Entrepreneurs engaged in jewelry, precious metals, works of art and antiques;

s) High-risk Clients who are assessed in the KYC process based on the risk arising from banking products, channels, profession, position and volume of transactions;

v) Entities whose beneficial owners are persons specified in subparagraph "j)" of this paragraph;

In the event of disagreement between the front office and the Compliance Control Department on the establishment of practical business relations with the client, the situation is escalated for consideration by the Supervisory Board of the Bank.

Establishing practical relations with persons related to offshore zones

83. For detailed information on the establishment of practical business relations of the Bank with citizens of countries and regions (offshore regions) where a preferential tax regime is provided and (or) financial transactions are not provided for, for disclosure and provision of information and control of transactions related to them, see Appendix H ***"Policy for Working with Offshore Territories" of this Procedure.***

XII. Specific Enhanced Due Diligence Requirements for Certain Customers

A) Politically Exposed Person (PEP)

84. When entering into a practical business relationship with a new customer, opening new accounts or carrying out transactions above a specified limit, the Bank is responsible for determining whether the customer is a PEP.

85. The following definitions are used to identify a PEP and related parties:

national political official - persons appointed or elected on temporary or special terms to legislative, executive, administrative or judicial authorities, including military structures, performing organizational and managerial tasks and authorized to perform legally significant actions, as well as political officials - heads of state-owned enterprises, prominent state politicians and prominent members of political parties (including former ones, from the date of whose departure from this position no more than five years have passed);

Foreign political official - persons appointed or elected to a permanent, temporary or special body in a legislative, executive, administrative or judicial body of a foreign state, including military structures, or international organizations, performing tasks of organizational management and having legal significance, authorized to perform such actions, as well as political leaders of foreign state enterprises, prominent politicians of a foreign state and prominent members of political parties (including former ones, from the date of whose departure from this position no more than five years have passed);

political officials of international organizations - heads, employees of international organizations or any person authorized to act on behalf of such an organization; family members of high-ranking officials - relatives of high-ranking officials include spouses, children, parents, brothers, sisters, including the parents of the spouse, as well as brothers, sisters and little sisters.

persons close to senior officials - publicly known individuals who maintain close relationships with senior officials, including individuals who have the ability to carry out significant domestic and international financial transactions on behalf of a politically exposed person (business associates, advisers, diplomats and assistants).

86. Customers who are defined as senior executives, whether individuals or legal entities, are considered high risk, regardless of geographic or other factors,

87. A bank shall use risk management systems to determine whether a customer or beneficial owner is a politically exposed person and, in conjunction with the necessary due diligence procedures for customers in relation to politically exposed persons or members of their families or close relatives of politically exposed persons acting as customers or beneficial owners, shall:

verify information about their position and take appropriate measures in the transaction to determine the sources of funds or other assets;

entering into practical business relations with him only with the permission of the Chairman of the Board of the Bank or his deputy, who has the appropriate authority (or continuation for existing clients);

it is necessary to regularly conduct in-depth monitoring of practical business relations.

88. All collected information must be documented in the client's KYC file. Front office employees generate the senior official form by obtaining additional documents confirming employment or status in the government organization to which the senior officials belong. In this situation, this Procedure applies (see Appendix F "Form of politically exposed persons")

89. The establishment of banking business relations with politically exposed persons or members of their families or persons close to politically exposed persons, or the continuation of relations with existing clients, is implemented after approval of the Chairman of the Management Board of the Bank or his deputy with the relevant authority, as well as the head of the Compliance Control Department.

90. If it is established that the client is no longer a politically exposed person (i.e. a former politically exposed person), the Bank will take effective measures to mitigate the residual risk for this politically exposed person. In accordance with the requirements of the risk-based approach, the Bank is required to confirm the following information by an undocumented method.

All registration processes must be documented.

the length of the person's tenure as a PEP; the extent of influence the person may still exert in government;

any connection between the person's previous responsibilities and his or her current employment/activities;

other credible information indicating a rational basis for deregistration as a PEP.

91. Risk mitigation measures shall be taken at least five years after the former PEP has left office.

92. In order to mitigate compliance risk, the Bank carries out daily checks of the Bank's existing customers (World Check Refinitiv) through the Surveillance System.

This check is carried out after the close of the Bank's business day.

The Compliance Control Department is responsible for monitoring the implementation of this process. In the event of identification of a new PEP among existing customers, after receiving permission from the Chairman of the Bank or his or her deputy with the relevant authority, he or she shall be granted a practical business relationship with the Bank.

B) Bank representative relationships

93. Correspondent bank relationships mean the provision of banking services by a Bank (the "correspondent bank") to the clients of another bank (the "respondent bank"). Correspondent banking does not include casual transactions or a simple exchange of SWIFT keys in the context of non-customer relationships, but is considered to be a type of business relationship of an ongoing, recurring nature.

94. In assessing the AML/CFT risks of a respondent bank, it is necessary to determine whether the Bank has taken into account all relevant risk factors and any risk mitigation measures to create a correct and complete picture of the risk of the respondent bank.

The Bank is obliged to carry out the necessary due diligence on a respondent bank that is its client, but is not obliged to carry out the CDD procedure in relation to the clients of the respondent bank. In the event that the Bank is invited to provide financial services as a respondent bank, the necessary due diligence on the respondent bank must be in accordance with the Bank's policy.

95. The Bank's Foreign Economic Activity Department is obliged to maintain a profile of all foreign clients of respondent banks. Before establishing representative relations with a respondent bank, it is necessary to study its system of combating ML/FT and CFMP based on a special questionnaire. This Procedure applies to this situation (see Appendix G "Questionnaire for establishing representative relations with a respondent bank").

96. Client profiles require the following: collection of information on the respondent bank in order to have full information on the specifics of its business activities;

determine, on the basis of public information, the reputation and quality of control of the non-resident bank, including whether or not investigative actions have been carried out in relation to violations of the fight against ML/FT and FPWMD in relation to this bank, and also determine whether any measures have been taken in relation to it by supervisory authorities;

whether measures have been taken in relation to the "transit accounts" of the respondent bank to carry out the necessary verification of its client, who has the opportunity to directly use the accounts of the correspondent bank, as well as the ability to provide information obtained as a result of the necessary identification of the client based on the request of the correspondent bank to receive the relevant confirmation;

store all information on electronic payments when establishing relations with other banks for the purpose of making transit transfers; ensure a clear and complete separation of responsibilities between correspondents. identification of the regulatory agency of the

client, which is the respondent bank; receiving and periodically updating the completed Wolfsberg questionnaire for the necessary verification of the respondent bank.

97. Under no circumstances may respondent banks enter into representative relationships with shell banks. The Bank shall also take appropriate measures to prevent shell banks from using respondent bank accounts. In order to ensure that a respondent bank is not a shell bank, the Bank should take the following measures:

• physical presence in the territory of the relevant jurisdiction;
• official recording of transactions;
• any full-time employees;
• regulation by the relevant authorities.

98. If there is information that non-resident bank accounts are used by banks that do not have permanent management bodies in the territories of their countries of registration, the Bank will take measures to prevent the establishment of relationships with them. Measures to continue representative relationships with respondent banks are carried out once a year.

99. The decision to establish representative relations between the Bank and a non-resident bank must be reviewed by the Compliance Control Department and the Bank's management and approved by the Bank's head.

XIII. Simplified Due Diligence (SDD)

100. Simplified Due Diligence (SDD) means that the required CDD measures are not required. In practice, the Bank carries out customer due diligence, i.e. the identification and verification process, when establishing a practical business relationship with a customer or in other cases.

However, Simplified Due Diligence (SDD) may be used for customers whose risks are considered low. In this case, the line of business staff may skip the verification process.

100.1. The Bank may apply the Simplified Due Diligence (SDD) procedure for the following customers:

a government agency, a local government agency, a public organization; regulated financial institutions; a publicly listed company duly listed on a stock exchange.

XIV. Regular Due Diligence

101. The front office staff conducts Periodic review for all customers and related parties as well as Event-driven review. The Periodic and Event-driven due diligence process includes a mechanism for identifying and verifying KYC information and re-assessing the customer's risk level, when necessary. The purpose of these processes is to determine whether the risk profile of customers has changed, whether customer information has been updated and whether any additional necessary due diligence measures have been taken.

A) Periodic review

102. All customers of the Bank are subject to periodic review for continuation of practical business relationship. The frequency of review depends on the risk level of the

Bank's customers. Customers with high, medium and low risk levels are subject to periodic review. The periodic review schedule for these customers is provided below:

Risk level	Periodicity
High Risk Clients	***1 y***
Medium risk clients	***2 y***
Low risk clients	***2 y***

103. The purpose of periodic due diligence is to review the risk level of the client and ensure that the client is operating in accordance with the client profile within the expected scope of activity and that the client identification information is up to date.

Any changes in the client risk rating (CRR) must be documented in the client KYC file with the rationale and actions taken. The periodic review period is monitored by the Compliance Control Department.

B) Event-driven review.

104. An event-based due diligence process may be performed prior to the next scheduled regular due diligence due to certain material events or changes related to the customer or related party.

"Material events" are any activity that may impact the overall ML risk of the customer, including relevant adverse news or changes in KYC information (e.g. jurisdiction, products, expected activity, purpose of the account, ownership structure and business structure).

105. There are many ways to detect material events or changes related to the bank's customer or related party (e.g. through monitoring, data provided by the customer or other sources).

In the event that the Line of Business or Compliance staff determine that a material incident has occurred in relation to the customer, they must notify the Compliance staff in accordance with the event-based review, which will then resume the regularly scheduled routine review.

106. Front office staff will conduct an event-based review process in the following instances:

Negative news is identified;
Penalties are applied (i.e., transactions are blocked or rejected);
One or more ODRs are notified;
Repetitive suspicious transactions;
Watch list system filtering process (due to a new addition to the Watch list system);
Criminal subpoenas or other law enforcement investigations;
Mergers or acquisitions with other organizations;
Changes in customer ownership or ownership structure;
Changes in customer control structure;
Changes in customer risk level;
Use of high-risk products or services.

107. The event-based review process may also include review of issues arising from the monitoring and reconciliation of transactions through the Watch List system. Any

incidents arising from these processes will be escalated to the Deputy Head of Compliance Control, which may result in an update of KYC information or a change in the customer risk rating.

B) Approval of Periodic and Event-based Review

108. Once the front office staff has completed the periodic and event-based review process for all customers and related parties, the bank will conduct the approval process in accordance with paragraph 54 of this Regulation to continue its operations.

XV. Third Party Involvement

109. A bank may rely on the necessary verification of a third party to carry out and complete the KYC process.

The bank must have an agreement with the third party ensuring that it meets the following criteria:

be able to obtain promptly the necessary information (via electronic systems) on the necessary customer verification measures;

be able to obtain promptly, upon request, a copy of the identification information and other relevant documents in connection with the necessary customer verification measures;

that the third party operates in accordance with internal controls to combat ML/FM and PFM, and They must ensure compliance with sanctions provisions and controls.

The third party must be located in the territory of the Republic of Uzbekistan.

110. In case of failure to meet one of the above requirements, the Bank will independently take measures to conduct the necessary verification of clients.

111. The third party is a person registered in Uzbekistan in the established manner and carrying out transactions with funds and other property, which include:

government services centers;

banks and other credit institutions; professional participants in the securities market;

stock exchange members; insurers and insurance brokers;

leasing organizations;

112. The Bank trusts and accepts the KYC process performed by third parties in the following cases:

identification and verification of the client's identity; identification and verification of the person acting on behalf of the client, based on the relevant documents; Identification and verification of the beneficial owner of the client.

113. In order to continue a contractual relationship with a third party, the Bank must annually assess the compliance of the KYC process implemented by that party with the Bank's Compliance Policy. To do this, the Bank must obtain all CDD information and documents from the third party and assess the necessary investigation. The Bank should also consider terminating trust in organizations that do not apply the CDD process or otherwise do not meet the requirements and expectations of customers.

In this case, the Bank should check and examine the terms of the contract concluded with the third party with a view to continuing the relationship with it.

XVI. Quality Control

114. To ensure that the KYC process is carried out in a quality manner in the Bank, the Bank conducts a quality control audit.

115. The quality control of KYC files is carried out once every quarter to assess the quality of customer interactions and the regular verification process, as well as to identify deficiencies in the KYC files or the need for additional training of line of business employees. Based on the methodology for assessing the risk level of clients, KYC files of low, medium or high risk clients are reviewed by the Compliance Control Department staff.

116. The quality control process may also be performed by a qualified third party (e.g. an external auditor). The Head of Compliance Control will pre-check the suitability and qualifications of the third party.

117. Upon acceptance of a new client or completion of a periodic review, the KYC file becomes part of the quality control content. Depending on the risk level of the client or specific types of clients, each appointed Quality Control Auditor is responsible for conducting the review in accordance with the following procedures.

The Quality Control Auditor shall receive a list of KYC files for the previous quarter when entering into practical working relationships with clients and when carrying out the regular verification process.

119. Based on the results of the checks, a quality control report shall be prepared and submitted to the Head of the Compliance Control Department. The results of the quality control check may be included in the agenda for discussion of the results at the expected meeting of the Bank's Management Board.

XVII. Storage and confidentiality of information and documents.

120. Documents related to the necessary customer verification, drawn up in whole or in part in a foreign language, must be requested by the Bank, where necessary, with a translation into the state language or Russian.

121. In the event of doubts about the correctness of copies of the submitted documents or if another need arises, the Bank has the right to demand the presentation of the original documents for review.

122. Information about the client obtained in the course of the necessary customer verification is recorded in his KYC form. In accordance with the internal documents of the bank, the client has the right to enter other information in the KYC form.

123. KYC forms for all clients (except for clients who do not require a comprehensive check) are filled out electronically using special software. The register of questionnaires of clients carrying out suspicious and/or questionable transactions and classified as high-risk is maintained in electronic form.

123.1. KYC forms completed electronically are stored in an electronic database that provides quick access to the Bank's employees for customer identification, as well as payment agents and payment subagents for checking information about the client.

124. The client's KYC form is stored by the Bank for at least five years from the date of termination of the relationship with the client.

125. Information about banking transactions, as well as identification data and materials of the necessary customer checks, account files and official correspondence, the

results of any analysis are carried out within the timeframes established by law, but after such transactions are carried out or must be stored for at least five years after the termination of practical business relations with clients.

125.1. These data and documents must be stored on paper and (or) on electronic media in a form that ensures timely submission to the competent government agencies and the Central Bank.

126. In order to limit the possibility of using documents used in the activities of the internal control service (correspondence with the Central Bank and the specially authorized state body, including electronic messages to the specially authorized state body, electronic KYC forms of clients, journals, etc.), such documents and their list must be directly stored in a room or safe specially equipped by the internal control service (responsible employee) for the periods established by law, but not less than five years.

127. The Bank restricts access to information, including documents stored in the Bank's archives, related to the fight against money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction, and ensures its non-proliferation, and legal entities and individuals do not have the right to inform a specially authorized government agency about the notification of their transactions.

128. The Bank ensures that information obtained in the course of performing internal control tasks is not disclosed (or used for personal purposes or in the interests of third parties) by its employees. Provision of information to third parties, including customer identification information from the KYC form, is carried out in accordance with the legislation

Annaxes

Information	Headline	File
Appendix A	KYC form for individuals	
Appendix B	KYC form for sole proprietors	
Appendix C	KYC form for legal entities	
Appendix D	Certificate of Beneficial Ownership	
Appendix E	Public Domain Search Methodology	
Appendix F	Form of a high-ranking official	
Appendix G	Questionnaire for establishing representative relations with respondent banks	
Appendix H	Policy for working with offshore zones	
Appendix I	Methodology for determining the beneficial owner of a client	