Internal Rules on Identification and Verification of Customers and Beneficiaries of "PASHA Bank" OJSC

1. General Statements

Internal Rules of "PASHA Bank" OJSC (hereinafter referred to as the "Bank") on Identifiaction and Verification of Customers and Beneficiaries (hereinafter referred to as the "Rules") have been prepared in order to determine the main principles of Compliance Policy of the Bank in accordance with the requirements established by the Law of the Republic of Azerbaijan "On Banks", Law of the Republic of Azerbaijan "On combating legalization of funds or other assets acquired by criminal means and financing of terrorism" (hereinafter referred to as the "Law"), normative acts of the Central Bank of the Republic of Azerbaijan and Financial Monitoring Service under the Central Bank of the Republic of Azerbaijan (hereinafter referred to as the "Financial Monitoring Service"), Charter of the Bank and "The Compliance Policy" of the Bank.

2. The Principle of "Know Your Customer"

2.1. One of the essential elements in risks management and minimization of the risk of losing business reputation of the Bank is the principle of "Know Your Customer" (hereinafter referred to as the "KYC").

2.2. Application of the KYC principle by the Bank pursues the purpose of ensuring compliance with the laws of the Republic of Azerbaijan, including legislation on combating legalization of income obtained through criminal means (money laundering) and financing of terrorism, compliance of the activities of the Bank to best practice of business and principles of professional ethics, as well as providing for the financial stability of the Bank.

2.3. In order to comply with the KYC principle, the Bank has prepared these Rules for carrying out bank transactions and other operations. All structural units of the Bank have to comply with the requirements of internal normative documents, including requirements concerning the KYC principle.

2.4. Programs on identification of the customers, determination and identification of beneficiaries, monitoring programs on cashflow through bank accounts are being developed and and applied in order to implement KYC principle in the Bank. The employees of the Bank have to support, within their functional duties, the Compliance Department of the Bank in implementation of the KYC principle, as well as any suspicious and/or unusual transactions discovered by such employees have to be fully and timely reported to them.

2.5. Through these Rules, the risk management system has been developed and applied in order to implement KYC principles.

2.6. The principle of KYC defines determination of rules for carrying out bank transactions and other agreements with customers and counterparties, including non-resident customers and counterparties, as well as determination of rules for running high risk bank transactions. Decisions on high risk bank transactions and other processes are made by management body of the Bank in complaince with the scope of authorities given by internal documents, and considering the degree of the that risk.

2.7. The KYC principle includes monitoring of cashflow through bank accounts and change of volume of cash in the bank accounts, monitoring of transactions associated with the high degree of risk and transfer of cash and other assets entrusted to the Bank for management, including taking of timely measures for managing typical bank risks (for example, credit, market, transactional, liquidity, legal and others), detection of suspicious transactions, as well as other operations of customers and counterparties undertaken by the Bank in order to discover any legalization of income obtained through criminal means (Money laundering) and financing of terrorism.

2.8. The main procedure in implementation of the principle of KYC is identifying the customers of the Bank (review of the client, verification of information about the client, maximum possible confirmation and justificationof information related to transactions and other operations of such customer, determination and identification of beneficiaries of transactions and other operations of the customer).

Customer indentification program, i.e.conditions for taking appropriate actions prior to establishing legal relations with customers, should be developed and implemented in order to provide environment for implementation of precautionary actions designated to reduce the risks.

In accordance with the Law of the Republic of Azerbaijan "On combating legalization of funds or other assets acquired by criminal means and financing of terrorism" dated February 10, 2009, in order to combat legalization of funds or other assets acquired by criminal means and financing of terrorism, identification of customers, determination and identification of beneficiaries are performed in compliance with these Rules.

Implementation of the KYC principle in the Bank presupposes the followings:

- Verification of accuracy of information filed by customers, counterparties, founders (shareholders);
- Review of documents defining the legal status of the customer and counterparty, as well authorities of individuals entering into an agreement;
- Determination of activity areas of customers and counterparties, analysis of information related to their business reputation, analysis of changes in reporting indicators, analysis of changes in activity areas of permanent customers and counterparties.At this time, high attention to the identificaton programme of customers using internet banking services are considered appropriate.

Depending on the nature and specifics of performed bank transactions and other operations (for example, attracting and placement of cash into deposits), expected continuity of contractual relationships with the customer, proposed volume of cash flow through the bank accounts (amount of the bank deposit) and other criteria, KYC principle considers the method for attracting customers and development of the customer identification program.

2.9. Special attention is paid to the customer identification in the Bank when relations are established with non-resident legal authorities.

2.10. During the creation of business relationships with legal entities, the Bank takes substantiated and feasible measures for the determination and identification of individuals who possess the capacity to exercise significant impact whether directly or indirectly(through third parties) upon decisions made by the governing bodies of credit organizations. .

3. Identification and verification of customer and beneficiary

3.1. The Bank must undertake the measures for the identification and verification of the customer as prescribed by Sections 3 and 4 of these Rules, and furthermore, identify the purpose and the beneficiary of business relationships in order to combat legalization of cash or other assets acquired through criminal means and financing of terrorism. Structural units and employees in the Bank directly working and communicating with the customers are responsible for the identification and verification of the customer and for the undertaking of the measures referred in this Rules. If any suspicious or an unusual circumstance is discovered in the course of customer identification and verification, the procedure of identification and verification of the customer must be transmitted to the relevant structural unit (Comliance Department).

3.2. The Bank must continuously update identification information of the customers of the Bank in existing business relationship.

3.3. The Bank can use any one or several methods for verification of the identification information with respect to the customer and beneficiary as stipulated in Clauses 3.9 and 3.10 of these Rules. As a rule, for the purposes of verification of information, used information must be obtained from sources which do not cause any doubts about their reliability, as well as independence of the sources (collection of information and documents from non-client sources).

3.4. The Bank, within the internal control system, may create an electronic database of documents referred in this Rules. For such purpose, one or more such documents are collected from the customer and photocopied and saved on electronic data carriers. The Bank can make the use of electronic information database for the purpose of verification of identification information related to the customer or the beneficiary.

3.5. The Bank must undertake the measures for the identification and verification of the customer and beneficiary in cases specified in Clause 3.2 of these Rules.

3.6. The Bank must take measures for identification and verification of new customers and must not engage any in any business relations prior to the adequate check of the identity of any new customers.

3.7. All required information for identificationof each new customer, determination of the purpose of businesss relations and specifics must be collected.

3.8. Considering characteristics of customer activities, the Bank must take measures for identification and verification of customers with whom business relationships have been estalished prior to these Rules,and who continue relationships with the Bank.

3.9. When the Bank fails to undertake identification and verification actions as prescribed by Section 3 of these Rules in relation to the customer, beneficiary or an authorized representative, and fails to collect information on the purpose and substance of business relationships of the customer with the Bank, the Bank must not carry on the relevant transaction, must not open an bank account, must not engage the customer, and when the required identification and verification cannot be performed following the establishmentof business relationships, must terminate such relationships and must disclose the relevant information to the Financial Monitoring Service.

4. Identification and verification of customers

4.1. It is prohibited for the Bank to open anonymous accounts, accounts for fictitious names and anonymous deposit accounts, to issue anonymous deposit certificates. Name of holder of any new account intended for opening, his major shareholders (founders) and persons with the signature authority or holders of powers of attorney must be verified within the "World-Check" system.

4.2. The Bank must undertake the measures for the customer identification in the following cases,:

4.2.1. prior to establishing business relations;

4.2.2. prior to any expected one-off transaction with amount of fifteen thousand manats (hereinafter - the limit) or over this amount (also, related to this case are, a series of several related transaction within the limit and with overall amount over this limit)

4.2.3. prior to the transfer of money without opening of an account irrespective of the amountof the transaction,

4.2.4. when there are circumstances raising a suspicion or providing sufficient grounds for suspicion that a transaction is associated with the acquiring the monetary fund or other assets through criminal means or financing of terrorism;

4.2.5. when there are revealed inaccuracies in the verification information previously submitted by the customer or beneficiary .

4.3. If the total amountof the transaction is not known prior to the executionof the transaction, identification of customer and beneficiary must be carried out at the time of when the amount of transaction is over thelimit.

4.4. Identification of a legal entity must be carried out on the basis of a notarized copy of his charter and a document on state registration of such legal entity. The Bank must require the submission of a notarized power of attorney issued to a person acting on behalf of a legal entityand must undertake measures for identification and verification of the autorized person. The Bank must identify registered address, legal organizational form, names of founders, as well as legal status of the legal entity on the basis of the charter and a document on state registration of the legal entity.

4.5. Identification of a physical person must be carried out on the basis of a personal identification document.

4.6. Identification of a physical person engaged into entrepreneurial activities without creation of a legal entity must be carried out on the basis of a personal identification document and the certificate issued by the relevant tax authority.

4.7. Copy of the personal identification document, as well as the certificate issued by the relevant tax authority, power of attorney evidencing the authorities of the representative, notarized copy of the charter and a document on state registration must be kept in the Bank.

4.8. In cases specified in Clause 3.2 of these Rules the Bank must undertake measures for the verification of identification information collected on customer and beneficiary by through reliable sources. The Bank must take measures for the determination of shareholders and management of a customer which is a legal entity. The Bank must also take measures for the determination of persons exercising control over a legal entity, real owners of a legal entity or individual ultimately controlling a customer which is a legal entity.

4.9. Measures related to the verification of legal authorities are as following:

4.9.1. comparison of the information submitted by the legal authority with the information maintained in the state register of legal authorities;

4.9.2. obtaining information on a legal authority from means of mass media, Internet information resources or formal publications;

4.9.3. comparison of any newly collected information with previously disclosed identification information .

4.10. Measures related to the verification of physical persons are following:

4.10.1. confirmation of date of birth based upon birth certificate, passport, driver's license or other formal document;

4.10.2. confirmation of the registered place of residence based upon receipts for payment of utility bills or fees for the use of non-residential premises, or extract on registration of title to property issued by the state immovable property register, confirmation of registration of residence on the basis of order, lease or rent agreement.

4.11. The Bank must collect information on the purpose and substance of business relationships with the Bank from the customer.

4.12. The Bank must take measures for the periodic updating of information collected with respect to commercial links and past transactions of the customer. The measures applied in relation to the periodic updating of information as carried out by the Bank are as following:

4.12.1. analysis of the past transaction for the purpose of determination of compliance thereof with the information related to the customer, his commercial activities and sources of income;

4.12.2. periodic updates of information and documents collected for identification of the customer through the analysis of information related to high risk customers or commercial relationships.

4.12.3 The Bank may apply a simplified identification and verification procedure with customer or beneficiary in cases referred to in Clauses 3.2.1 and 3.2.2 of these Rules. Rules on simplified identification and verification procedure are prescribed by the Financial Monitoring Service based upon investigations related to the customer, commercial relationships or sources of income.

5. Identification and verification of the customer based on risk and high risk based approach

5.1. The Bank must apply further identification procedures with respect to the high risk customers in addition to identification and verification procedures prescribed by Clause 3 of these Rules. In case of determination and evaluation of risks related to the legalization of monetary funds or other assets acquired through criminal means and financing of terrorism, the Bank must take into account the following types of risks:

- State risk;
- Customer risk.

5.2. State risk:

5.2.1. When the Bank evaluating the risk of any state in relation to the legalization of monetary funds or other assets acquired through criminal means and financing of terrorism, the system and financial environment of such country designed to combat legalization of monetary funds or other assets acquired through criminal means and financing of terrorism is taken as basis.

5.2.2. Transactions with states (territories) whose list was determined and published by the Financial Monitoring Service in accordance with the procedure prescribed by the legislation, states which are believed to be engaged into legalization of monetary funds or other assets acquired through criminal means, financing of terrorism, transnational organized crime, armed separatism, extremism and hired combatants, illegal circulation of drugs and psychotropic substances must be deemed to be high risk transactions.

5.3. Customer risk:

5.3.1. The Bank must evaluate the risks related to the legalization of cash or other assets acquired through criminal means and financing of terrorism depending on specifics of the customer in accordance with Clause 4.1 of the Rules. During the evaluation of risks, such factors as occupation of customers, nature of a transaction and periodicity of operation must be taken into account. The Bank must treat the following categories of customers as high risk customers:

5.3.1.1 Politically exposed persons of any countries;
5.3.1.2 Non-resident customers;
5.3.1.3 . legal entities entrusted with the right for the management of cash, securities or other assets;
5.3.1.4 legal entities acting as nominal holders or issuers of bearer shares;
5.3.1.5 Persons included in the list approved by the Financial Monitoring Service; www.fiu.az/persons-to-be-imposed-sanctions
5.3.1.6 citizens of states (territories) included in the list approved by the Financial Monitoring Service, individuals having place of registration, place of residence or place of main activity in such states (territories), as well as persons having account in banks registered in such states (territories). www.fiu.az/countries-that-do-not-cooperate

5.4. Politically exposed persons of any countries

5.4.1. Politically exposed individuals refers to individuals who hold or held an important public post in any state (heads of state and government, influential politicians, members of the government, judges of higher level courts, high ranking military servants, officials of state owned enterprises, officials of political parties), as well as family members and close relatives of an individual who holds or held an important public post in any state.

5.4.2. In order to determine the fact whether an individual is or is not a politically exposed individual,the relevant information must be collected from every new customer, and such information must be verified through open information sources and special electronic information databases.

5.4.3. The citizen of any state must be required to complete a form on opening and managing accounts provided in the Appendix to relevant Rules in order to facilitate the determination process of the status of a politically exposed individual.

5.4.4. The Bank must regularly review its existing business relationships with politically exposed persons, must undertake measures for periodic updating of identification and verification documents.

5.4.5. The Bank must undertake additional identification activities with respect to the politically exposed persons in accordance with the Clause 7 of these Rules.

5.5. Non-Resident Customers

5.5.1. Special attention of the Bank must be paid to the business relationships with nonresident customers.

5.5.2. Bases for opening bank accounts in the Bank by non-residents, as well as transactions related to operations with monetary funds and other assets must be investigated by the Bank.

5.6. Establishment of correspondent bank relationships, "Shell-Banks"

5.6.1. The Bank must apply additional identification measures as prescribed by Clause 4.7.2 of the Rules in relation to transactions performed through accounts maintained by foreign correspondent banks.

5.6.2. The foreign bank must be required to complete a self-evaluation questionnaire (Appendix 2 to these Rules) when opening a correspondent account for a foreign bank. Such questionnaire must be reviewed by the Bank officials and a report on results of such review must be provided to the Bank's officer (Chairman of the Executive Board).

5.6.3. The Bank may disclose to the Financial Monitoring Service information on reasons for the refusal to open correspondent accounts for foreign banks.

5.6.4. Correspondent accounts of foreign banks can be opened in a local bank only upon consent of the Chairman of the Executive Board of the Bank.

5.6.5. It is not permitted to the Bank to establish or maintain relationships with shellbanks through the mean of opening the correspondent accounts. The Bank must be assured that its counterparty foreign financial institutions do not permit the use of accounts by shell-banks.

5.7. Identification and verification of customers (risk and high risk based approach)

5.7.1. In addition to the actions on identification and verification of customers as prescribed by Clause 3 of these Rules, the Bank must apply further identification measures with respect to the following high risk transactions:

5.7.1.1. transactions with non-resident customers;

5.7.1.2. transactions with legal entities entrusted with the duty for the management of monetary funds, securities or other assets;

5.7.1.3. transactions with legal entities acting as nominal holders or issuers of bearer shares;

5.7.1.4. transactions carried out via correspondent accounts with foreign banks;

5.7.1.5. circumstances raising a suspicion or providing sufficient bases for suspicion that a transaction is associated with the acquisition of monetary funds or other assets through criminal means or financing of terrorism;

5.7.1.6. any transactions with monetary funds or other assets by citizens of states (territories) included within the list made by the Financial Monitoring Service and submitted to the Bank,

persons having place of registration, place of residence or place of main activity in such states (territories), as well as persons having account in banks registered in such states (territories);

5.7.1.7. transactions with monetary funds or other assets of politically exposed persons;

5.7.1.8. transfers of monetary funds from anonymous accounts from outside the jurisdiction of the Republic of Azerbaijan or transfers to anonymous accounts situated outside the jurisdiction of the Republic of Azerbaijan;

5.7.1.9. transactions with persons mentioned on the list approved by the relevant executive authority with the reference to the relevants resolutions of the United Nations Organization, the legislation and international treaties of the Republic of Azerbaijan.

5.7.2. Additional identification measures as applied by the Bank are the following:

5.7.2.1. checking of accounts and business relationships, or clarification of the purpose and substance of transaction through other means;

5.7.2.2. obtaining information on shareholders of the customer whis is a legal entity and their holdings;

5.7.2.3. collection and comparison of more accurate information on customer, beneficiary and whene possible, sources of monetary funds or other assets from other reliable sources.

5.7.2.4. If it is not possible to identify the transacting parties in accordance with the procedure prescribed by these Rules or a customer or a beneficiary refuses to provide information required for identification, or it is revealed that information previously provided by the customer or beneficiary is inaccurate, the Bank must not carry on the relevant transaction, must not engage in business relations, must not open an account and must disclose the relevant information to the Financial Monitoring Service.

5.8. Classification of customers into risk categories and maintaining the lists.

5.8.1. All customers of the Bank are classified on risk criteria into the following categories:

- Low-risk customers (additional register is not conducted, it includes ordinary customers, ie not attributed to the categories below);
- Medium-risk customers (it includes customers suspected for any reason and register on them is conducted);
- High-risk customers (it includes customers with suspicion that have been confirmed, as well as those mentioned below and register on them is conducted):
    - Non-resident (also a non-resident person acting on the base of letter of attorney);
    - Politically exposed person (when a potential customer declares to be a politically exposed person in the survey or when the customer's name is identified by the World Check system as a politically exposed person);
    - Legal entity identified as having difficult and chain ownership structure;
    - Legal entity identified as having in the ownership structure any natural or legal entity who is a resident of the United States.

5.8.2. Renewal of documentation related to the customers included in the risk categories should be carried out by the Department of Compliance. Documentation of high-risk customers should be renewed once a year, documentation of medium-risk customers should be renewed once in 2 (two) years. Renewal of low-risk customers´ documentation is carried out once in 3 (three) years by structural division executing functions of customer care. Renewal means that the documentation should be reviewed, the period of validity of the documents should be checked and verification measures should be carried out if necessary.

5.9. Specific requirements according to the fields of activity are the following:

5.9.1. The Bank distinguishes its customers in specific risk categories according to the fields of activity. Some fields of activity of customers are considered risky or high risk by the Bank.

5.9.2. The following fields of activity are considered medium risk by the Bank and are included in the Medium-Risk customers` register:

- Companies engaged in oil and gas production and sales;
- Companies engaged in coal and metal production and sales;
- Companies engaged in medications manufacture and sales;
- Companies engaged in precious metals (gold, silver, platinum and precious stones) production and sales.

5.9.3. The following fields of activity are considered high risk by the Bank and are included in the High-Risk customers` register:

- Financial Institutions;
- Companies dealing with money transfer;
- Companies engaged in the manufacture and sale of arms;
- Casino, gambling, and totalisator agencies;
- Legal entity managing the entrusted cash, securities or other property (investment funds, legal entities providing dealing and broker services etc.);
- Financial institutions (banks, credit organisations, credit unions etc.);
- Legal entity being a nominal holder or issuer of bearer shares.

6. Continuous monitoring of customer accounts and transactions carried out by them

6.1. Considering the specifics of activities of the customers, the Bank must undertake actions for the identification and verification of customers with whom business relationships have been estalished prior to the effective date of these Rules and continue at the present time.

6.2. Considering the specifics of activities of the Bank, in accordance with the procedure specified by the legislation, the Bank may require the disclosure of additional documents related to the identification of the customer and of the beneficiary.

6.3. Accounts and transactions of customers must be continuously monitored.

6.4. The Bank must monitor compliance of transactions of customers with the purposes of business relationships.

6.5. The Bank must determine the periodicity of the monitoring based on the level of risk posed by the transactions.

6.6. Monitoring must be carried out based upon risks for the purpose of determination of unusual and suspicious transactions. The following minimum components must be taken into account in course of monitoring in relation to the existence of unusual or suspicious transactions:

6.6.1. Establishment of limits for certain categories of accounts and transactions and detection of transactions carried out in excess of such limits;
6.6.2. Verification of compliance of the commercial activities area of the Bank’s customer with the transactions of such customer;
6.6.3. Detection of transactions without an economic or commercial purpose or depositing to the accounts of large amounts of cash or other assets not in line with the ordinary and expected operations of the customer.

6.7. The monitoring of high risk transactions must be of higher intensity. Depending on the source of funds, country of their origin, associated categories of transactions and other similar risk factors, special indicators relevant to such transactions must be established.

6.8. Continuous monitoring over the purpose and substance of business relationships of the existing customers must be carried out.

7. Establishing business relationships by means of technological methods without personal contact

7.1. In course of establishing business relationships by means of technological methods without personal contact as well as while performing identification and verification of such customers, the Bank must carry out the aforementioned actions and procedures. Therefore, the following minimum actions must be undertaken:

7.1.1. to implement verification measures for the purpose of specifying the personality of the proposed customer.

7.1.2. to implement verification measures for the purpose of determination of actual place of residence of the proposed customer.

8. Final Statements

8.1. These Rules shall come into legal force upon approval by the Bank's Supervisory Board.

8.2. *Compliance Department* can make changes to Appendixes of these Rules based upon new compliance risks, any relevant changes and activities in the structure of the Bank. These kind of changes are not subject to approval by Supervisory Board of the Bank.

8.2 Current Rules must be reviewed not less than once a year . Extraordinary reviews must be held if any changes occur in the Legislation.

Appendix No. 1 to PASHA Bank OJSC Internal Rules on Customer Identification and Verification

GENERAL INFORMATION

1. Name of Financial Institution (FI):
2. Legal Address:
3. Contact name, phone, email address:
4. Type or Description of Identification document, including name of authority issuing the ID:

5. Amount of total assets (audited figures):
6. Form of legal entity:
7. Ranking of FI:
8. Registration number:
9. Date of registration:
10. Number of employees:
11. Are shared of your institution (or parent company) listed in stock exchange? ☐Yes ☐No

If yes, on which stock exchange(s) are your shares listed?

12. Please confirm the areas of your organization covered by this questionnaire:

- AML questionnaire applies to this branch/subsidiary only ☐Yes ☐No
- Head Office & Domestic subsidiaries ☐Yes ☐No
- Domestic subsidiaries ☐Yes ☐No
- Overseas branches ☐Yes ☐No
- Overseas subsidiaries ☐Yes ☐No

13. How many branches does FI currently have?

14. How many LORO correspondents do FI currently have?

Please list below or attach to this questionnaire a LİST (if there is no additional space) of all your LORO correspondents, including the Name, Address, Country.

№	***NAME***	***ADDRESS***	***COUNTRY***
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

QUESTIONS RELATED TO REGULATORY ENVIRONMENT

15. Are your institution's AML/CTF policies and practices being applied to all foreign branches and/or subsidiaries and/ or separate legal entities in the home country or in locations outside of that jurisdictions:

16. Is your institution operating as an Offshore Banking Unit? ☐Yes ☐No

- Does your institution have any branches, subsidiaries or affiliates operating as an Offshore Banking Unit? ☐Yes ☐No

17. Is your institution fully compliant with anti-money laundering and terrorist financing laws in your country? ☐Yes ☐No

QUESTIONS RELATED TO YOUR INSTITUTION'S AML/CTF POLICIES AND PRACTICES

18. Does your FI have a requirement for independent audit or testing of anti-money laundering compliance program? ☐Yes ☐No

- *If Yes, how frequently are these audits/tests conducted?*
  Monthly ☐
  Quarterly ☐

Annually ☐
Other ☐

19. Name of Auditing Company or Department:

20. Does your FI have policies that prohibit your institution from opening anonymous accounts? ☐Yes ☐No

21. Does your FI have a written policy, controls and procedures designed to prevent and detect money laundering/terrorist financing activities? ☐Yes ☐No

22. Does the FI have policies and procedures against establishing and maintaining business relationships with shell banks? ☐Yes ☐No

23. Does your institution's AML/CTF policy and program include the following:

- Does the FI have an officer-in-charge for enforcing AML/CTF policies and procedures? ☐Yes ☐No
- Does A requirement for periodic approval of your institution's AML/CTF policy by your institution's Board or senior committee exist? ☐Yes ☐No
- Does your FI have specific identification requirements for the sale of monetary instruments or wire transfers? ☐Yes ☐No

  (If a specific limiting amount is established for such transactions, please specify):

- Compliance with local suspicious activity reporting requirements? ☐Yes ☐No
- Procedures to monitor large cash deposits and withdrawals? ☐Yes ☐No
- Record retention requirements for documentation obtained regarding customer identification? ☐Yes ☐No
  (If Yes, how long are records retained?)
- Policies covering relationships with politically exposed persons, their families and close associates consistent with regulations existing in your country? ☐Yes ☐No
- Risk rating of your customers and products? ☐Yes ☐No
- Requiring a higher level of due diligence for high risk clients (i.e. those parties presenting risks of illicit activities, including but not limited to money laundering, fraud or terrorist financing)? ☐Yes ☐No
- Has the FI implemented data documentation and confidentiality policies and procedures in accordance with existing laws on AML/CTF? ☐Yes ☐No
- Does the FI have a program for monitoring unusual or suspicious transactions involving the transfer of cash, travelers checks or other financial instruments transfers in place? ☐Yes ☐No

24. Does your FI provide services to the following:

- Financial Institutions located outside of your country ☐Yes ☐No
- Offshore Banking Units ☐Yes ☐No
- Internet Banks ☐Yes ☐No
- Casino and Gambling businesses ☐Yes ☐No
- Companies providing money transfers ☐Yes ☐No
- Companies who are nominal holders of or have issued =bearer shares ☐Yes ☐No

AML/CTF TRAININGS

25. Does the FI hold employee training sessions on the following topics:
- Detecting and submitting transactions to be reported to financial monitoring authorities; ☐Yes ☐No
- Various classifications of AML/CTF, covering the bank's products and services; ☐Yes ☐No
- Policies on AML/CTF; ☐Yes ☐No

26. Does the FI retain information on the seminars it holds, including the respective seminar materials and notes on attendance; ☐Yes ☐No

27. Are the bank's employees notified of changes and amendments to current AML/CTF laws? ☐Yes ☐No

28. Does the FI involve any third parties in its activities? ☐Yes ☐No

29. Does the FI hold training sessions on the following for any third parties involved in its activities:
- Detecting and submitting transactions to be reported to financial monitoring authorities ☐Yes ☐No
- Various classifications of AML/CTF, covering the bank's products and services; ☐Yes ☐No
- Policies on AML/CTF; ☐Yes ☐No

IDENTIFICATION, VERIFICATION AND ADDITIONAL IDENTIFICATION

30. Does the FI have procedures that detect the real identity behind accounts managed by another person or through which another person is performing transactions? ☐Yes ☐No

31. Does the FI require that detailed information is collected concerning the business activities of customers? ☐Yes ☐No

32. Does the FI have procedures in place for recording and cataloguing documents on each new customer, to include identification, verification and background check information? ☐Yes ☐ No

33. Does the FI evaluate its customers' experience, policies and procedures related to AML/CTF? ☐Yes ☐No

34. Does the FI have procedures for continuously monitoring and updating information on high-risk customers? ☐Yes ☐No

DETECTING, PREVENTING AND REPORTING SUSPICIOUS TRANSACTIONS

35. Does the FI have procedures and experience in detecting and transmitting transactions that are to be reported to financial monitoring agencies? ☐Yes ☐No

36. Does the FI have procedures to detect in place operations designed to deviate the reporting requirements on cash transaction information? ☐Yes ☐No

37. Does the FI cross-check customers and transactions against the watch list of individuals and countries issued by financial monitoring authorities? ☐Yes ☐No
(If yes, please specify which sanction lists?)

38. Does the FI verify that its correspondent banks are properly licensed to do business in their respective countries? ☐Yes ☐No

GENERAL COMPLIANCE QUESTIONS

39. Do you comply with FATF Special Recommendation VII? ☐Yes ☐No

40. Has your FI had any regulatory or criminal enforcement actions resulting from violations of anti-money laundering laws or regulations in the past five years? ☐Yes ☐No
If Yes, please provide an explanation.

41. Has your FI, to your knowledge, been the subject of any investigation, indictment, conviction or civil enforcement action related to financing terrorists in the past five years? ☐Yes ☐No

- *If Yes, please provide an explanation*

42. Do you conduct any banking transactions with non-established customers or walk-ins (non-account holders)? ☐Yes ☐No

- *If Yes, how does your institution mitigate the risk associated with these non-account holders?*

43. We hereby comfirm that we do not open any shell-bank accounts, nor do we perform any transactions directly in favor of such banks, or use any products offered by them.
☐Yes ☐No

OWNERSHIP AND MANAGEMENT

44. Please provide below the full ownership structure of your bank.

45. PLEASE MAKE SURE TO INDICATE NAME ADDRESS AND PERCENTAGE of ownership for BOTH direct as well as indirect (beneficial) owner of your bank with *(Additional information can be attached to the questionnaire)*

№	***Name***	***Type of owner(direct\indirect)***	***Type of Entity (legal entity or individual)***	***Date of Birth (individual)***	***Address***	***% of ownership***
1						
2						
3						
4						

5						

46. Does beneficial owner (s) have passport/ green card/residence permit of USA? [*if YES, please provide a copy]* ☐Yes ☐No

47. Please provide the names, titles, date of birth and country of residence of the members of Senior Management and of the members of Supervisory Board (Board of Directors) *(Additional information can be attached to the questionnaire)*

Supervisory Boar (Board of Directors):

- Please make sure to identify the Chairman, Secretary and all board members

№	***Name***	***Title***	***Date of Birth***	***Country(citizenship)***
1				
2				
3				
4				
5				

Senior Management:

- Please make sure to identify equivalent of the following titles: Chairman of the Executive Board CEO (Chief Executive Officer), Members of the Executive Board, CFO (Chief Financial Officer), COO (Chief Operating Officer) and etc. *(Additional information can be attached to the questionnaire)*

№	***Name***	***Title***	***Date of Birth***	***Country (citizenship)***
1				
2				
3				
4				
5				

- To the best of your knowledge, do any politically exposed persons have a controlling interest or executive management role in the institution? ☐Yes ☐No

  If yes, provide their full legal name, address, date of birth, percentage of ownership (if owner) and role in the institution below: (Additional information can be attached to the questionnaire)

	Name	***Address***	***Date of Birth***	***Role***	***Owners***

№					***hip (%)***
1					
2					
3					
4					
5					

- Have there been any recent (i.e. within the last 5 years) material ownership changes or recent material changes in the Executive Board structure (e.g. within the last 2 years)? ☐Yes ☐No
  If yes, please briefly describe below these changes

Use this space to provide additional information (Please include the number of the question for which you are providing additional details)

NAME:
JOB TITLE:
EMAIL:
SIGNATURE:
DATE: