Brillink Bank

Anti-Money Laundering and Counter-Terrorist Financing Policy

Version	Last updated by	Last updated date	Approved by
0.0	Newly established	13/04/2021	Board of Directors
1.0.	Update by CCO	13/06/2022	Board of Directors

Article 1. Definitions

1. The following concepts and abbreviations are used in this Policy of Bank and its subsidiaries on combating the legalization (laundering) of proceeds from crime and financing of terrorism (hereinafter - "AML/CTF Policy"):

1) **AML/CFT** – anti-money laundering, countering the financing of terrorism and the proliferation of weapons of mass destruction;

2) **beneficial owner -** an individual who:

directly or indirectly owns more than twenty five (25) percent of interest in the authorised capital or placed shares (less preferred shares and shares redeemed by the company) of the Customer – entity,

an individual exercising control over the Customer in another way;

or in behalf of which the Customer performs operations with money and (or) other property;

3) **Customer** – an individual or legal entity receiving the Bank's services;

4) **CDD**– customer due diligence **-** a set of procedures for identifying the Bank's customers aimed at collecting, studying and analysing information about the Bank's customers in order to prevent and identify actions related to the ML/FT;

5) **FIU -** Financial Intelligence Unit – authorised state body a state body that carries out financial monitoring and takes other AML/CFT measures in accordance with the AML/CFT Law;

6) **FATF -** the Financial Action Task Force on money laundering (FATF) - the intergovernmental organization, developing the recommendations in the area of combatting money laundering and the financing of terrorism;

7) **legalisation (laundering) of proceeds from crime** – involvement of money and (or) other property in the legal circulation, obtained by criminal means, through the execution of transactions in the form of conversion or transfer of property generating income from criminal offences, or possession and use of such property, concealment or disguise of its true nature, source, location, manner of disposition, relocation, rights to property or its ownership, if such property is known to represent the proceeds from crime, as well as the mediation in legalisation of money and (or) other property obtained by criminal means;

8) **legislation on AML/CFT–** legislation of the Republic of Kazakhstan and AIFC on AML/CFT;

9) **ML/FT risk management** - a set of measures taken by the Bank to identify, assess, monitor and minimise the ML/FT risks (in relation to products/services, Customer, and/or transactions performed by Customer);

10) **ML/FT -** money laundering and the financing of terrorism – the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction;

11) **MLRO -** Money Laundering Reporting Officer – a person with responsibility for implementation and oversight of its compliance with the AML Rules, who has an appropriate level of seniority and independence to act in the role;

12) **suspicious operation -** a suspicious transaction with money and (or) other property – an operation of the Customer (including an attempt to perform such an operation, an operation

in progress or a completed operation), in respect of which there are suspicions that the money and (or) other property used to perform it are proceeds from crime, or the operation itself is aimed at the legalization (laundering) of proceeds from crime or financing of terrorism or other criminal activity;

13) **threshold transaction** - a transaction with money and/or other property subject to financial monitoring in accordance with national legislation;

14) **the "AFSA" -** the Astana Financial Services Authority;

15) **the "AIFC" -** the Astana International Financial Centre;

16) **the Bank** - Brillink Bank Corporation Limited;

2. Other terms and definitions used in the Policy are used in the meaning established in the legislation on AML/CFT and the internal normative documents of the Bank.

Article 2. The General Provisions

3. The AML/CTF Policy is drafted in accordance with the legislation on AML/CFT, FATF recommendations, international standards, best international AML/CFT practice.

4. The purpose of the AML/CTF Policy is to create an internal control system in the Bank for AML/CFT purposes, to prevent the involvement of the Bank and their employees in operations related to the ML/FT. For these purposes, the Bank has agreed:

1) to follow the provisions and approaches set out in the Policy when creating and improving the internal control systems for AML/CFT purposes;

2) to develop their own internal control rules and procedures for AML/CFT purposes on the basis of the legislation on AML/CFT and unify them with the standards set out in the Policy;

3) to take actions aimed at mitigating the risks associated with the involvement of the Bank and their employees in the ML/FT;

4) maintain the effectiveness of the internal control system of the Bank at a level sufficient for the management of the ML/FT risks and associated risks (operational, reputational, legal);

Article 3. Organisation of internal control for AML/CFT purposes

5. Organisation of the internal control system for AML/CFT purposes is based on the risk-based approach (RBA) and compliance with three (3) lines of defence in risk management related to the ML/FT, where:

1) first line of defence is all employees of the Bank;

2) second line of defence is MLRO/ the employee(s) or division whose competence would include AML/CFT issues (hereinafter -the AML/CFT Function);

3) third line of defence is an internal audit subdivision that evaluates the effectiveness of the internal system of AML/CFT.

6. When creating and maintaining the internal control system for AML/CFT purposes, the Bank proceed on the basis that:

1) responsibility for the creation and effective operation of the internal control system for AML/CFT purposes lies with the Senior management of the Bank;

2) all employees of the Bank, within their competence, are responsible for the existence and functioning of the internal control system for AML/CFT purposes, and participate in the activities aimed at implementing the provisions of the Policy;

3) in accordance with the procedure established by legislation on AML/CFT, the Bank must ensure the appointment of MLRO;

4) all employees should be aware of and understand their responsibilities and duties arising from the provisions of the regulatory acts of the legislation on AML/CFT;

5) the Senior management of the Bank is regularly, in accordance with the deadlines determined by the legislation on AML/CFT and (or) the internal normative documents, provided with information on the effectiveness of internal control system on AML/CFT when managing the risks;

6) for AML/CFT purposes, the Bank uses an automated information system to identify threshold transaction, including suspicious transactions, and to send relevant data and information to the FIU in a timely manner;

7) the Bank has the internal normative documents on internal control issues for AML/CFT purposes, including:

a) procedures for identifying the Customers and monitoring of activities of the Customers;

b) procedures for screening Customer's and bank's transaction against sanctions lists – official documents that contain the names of individuals, groups and organisations against which economic or legal restrictions are directed, developed by Republic of Kazakhstan or authorised international organisations and states;

c) risk management procedures and methodology for assessing and monitoring ML/TF risks;

d) provisions on the reporting of information to the FIU and protection of information;

e) provisions on the storage of official information;

f) provisions on ensuring the confidentiality of information;

g) procedure for training employees;

h) requirements for the appointment, qualification and training of employees of the AML/CFT Function;

8) the documents defining the implementation of internal control for AML/CFT purposes are regularly reviewed in order to align them with the changed requirements of the legislation on AML/CFT, new products and/or other changes in the activity of the Bank.

Article 4. The functions of the MLRO and AML/CFT Function

7. The Bank appoints an individual as MLRO, with responsibility for implementation and

oversight of its compliance with the AML Rules, who has an appropriate level of seniority and independence to act in the role.

8. MLRO an individual invited to perform that function must be individually approved by the AFSA on the application by the Bank. MLRO will need to meet the fit and proper criteria for Approved Individuals and have appropriate level of seniority and independence to act in the role.

9. The Bank also determines the AML/CFT Function. In this case, the MLRO performs managerial functions, and the AML/CFT Function performs executive functions.

10. The functions of the MLRO or the AML/CFT Function:

- implementation of the legislation on AML/CFT and international AML/CFT standards;
- organisation of reporting and control over the reporting to the FIU in accordance with the AML/CFT Law and promptly notifies the AFSA of such a submission;
- other functions established by the legislation on AML/CFT and internal normative documents of the Bank.

Article 5. ML/FT risk management

11. For the purposes of ML/FT risk management a risk assessment program is being developed in the Bank, according to which the structure and functional duties of employees are determined, ML/FT risks assessment methodology is developed and the procedure of assigning, timing and grounds for reviewing the level of ML/FT risks, the procedure for recording, accounting ML/FT risks, control measures and procedures for management and mitigation of ML/FT risks and the procedure for verifying the effectiveness of ML/FT risk management program are determined.

12. The Bank takes appropriate steps to manage and mitigate country wide risks, including those relevant for the Republic of Kazakhstan identified in the published reports and guidance given by the FIU regarding the FATF mutual evaluations and follow-up reports, and implement enhanced measures where higher risks are identified.

13. In order to identify and assess the ML/FT risks the Bank conducts a business risk assessment and also conducts customer risk assessments and keeps these assessments up to date.

14. For the purposes of mitigating ML/FT risks, the Bank in accordance with the legislation and international standards in the area of AML/CFT take the following measures:

1) prohibit the opening and maintenance of accounts (deposits) for anonymous owners, as well as the opening and maintenance of accounts (deposits) for owners using fictitious names (aliases);

2) prohibit the opening and maintenance of correspondent accounts of banks that do not have a physical presence and (or) any permanent management bodies (Shell Bank) on the territory of the countries in which they are registered, or a bank which is known to permit its accounts to be used by Shell Banks;

3) prohibit the conducting transactions with designated persons and entities, as per the obligations set out in the relevant resolutions or sanctions issued by the United Nations Security Council ("UNSC") or by the Republic of Kazakhstan;

4) prohibit the opening and maintenance of correspondent accounts of banks registered in foreign countries (territories) included in the list of states (territories) not performing or inadequately performing FATF recommendations;

5) prohibit or perform a special enhanced financial monitoring when servicing foreign trade contracts, receiving payments and transfers in foreign currency for execution with the participation of Customers and (or) counterparties who are residents of foreign states (territories) included in the list of states (territories) not performing or inadequately performing FATF recommendations, respectively;

6) check Politically Exposed Person ("PEP") and/or members of his family and close relatives for his/their involvement in the cases of ML/FT when establishing/continuing business relations, performing transactions (deals);

7) prohibit establishing business relations with the Customer (the Customer's representative), if they do not provide the documents and information required by the legislation on AML/CFT for identification;

8) where, in relation to any customer, the Bank is unable to conduct or complete the requisite CDD in accordance with verification of obligations it must, to the extent relevant:

- not carry out a transaction with or for the customer through a bank account or in cash;

- not open an account or otherwise provide a service;

- not otherwise establish a business relationship or carry out a transaction;

- terminate any existing business relationship with the customer;

- consider whether the inability to conduct or complete CDD necessitates the making of a suspicious operation report;

9) draft and approve of internal normative documents on AML/CFT and update them in a timely manner in accordance with amendments to the legislation on AML/CFT;

10) use and improve the automated information system for AML/CFT purposes;

11) maintain a RBA to the examination and analysis of operations of the Customer for detecting suspicious transactions;

12) take measures to reduce the risk level, up to the termination of business relations with the Customer if the latter uses banking products and services to execute transactions for the purposes of ML/FT;

13) train and test the knowledge of employees of the Bank on AML/CFT;

14) take other actions for AML/CFT purposes.

Article 6. Customer Due Diligence

15. For CDD (and/or their representatives) and any beneficial owners the Bank records information about the customer (its representative), the beneficial owner of the customer and the intended purpose and nature of business relations of the business relationships before establishing business relationships. It must include the receiving and recording relevant information by using the AML/CFT Law on the customer (and/or its representative) and the beneficial owner or owners.

16. The Bank chooses between the Standard Due Diligence and the Enhanced Due Diligence, depending on the client's risk level, in accordance with the AML/CFT Law.

17. Information received in the framework of the customer identification (its representative) documented and included in the Customer's profile. It is kept by the Bank throughout the entire period of business relationships with the customer and for at least six years after the day of termination of the business relationships.

18. The frequency of updating and/or the need to obtain additional information on the Customer (its representative) and the beneficial owner established taking into account the level of risk of the Customer (group of clients) and/or the degree of exposure of the services (products) of the Bank provided to the Customer to ML/FT risks. Information on each high risk Customer (or its representative) and the beneficial owner (s) updated by the Bank at least once a year.

19. The Bank relies on the following third parties to conduct one or more elements of CDD on its behalf:

1) an Authorised Person;

2) a law firm, notary, or other independent legal business, accounting firm, audit firm or

insolvency practitioner or an equivalent person in another jurisdiction;

3) a Regulated Financial Institution; or

4) a member of the Relevant Person's Group

20. The existence of the consent of the customer to the gathering, processing, storage and provision, including, if necessary, to third parties of his/her personal data, confirmed by an identification tool is obligatory for the Bank.

21. The Bank relies on a third party only if extent that:

1) immediately obtains the necessary CDD information including Customer and beneficial owner identification and verification documents, and information on the purpose and nature of the business relationship or transaction from the third party;

2) the third party has taken necessary measures within the scope of CDD, particularly, customer identification and record keeping;

3) takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of CDD will be available from the third party on request without delay. It is deemed sufficient that the third party certifies the customer identification documents as "the true copy of the original";

4) regular assurance testing is carried out in respect of the third party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient;

5) the person in AML 9.1.1(b) to (d) is subject to regulation, including AML regulation, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations;

6) the third party has not relied on any exception from the requirement to conduct any relevant elements of CDD which the Bank seeks to rely on; and

7) the information previously obtained by a third party which covers one or more elements of CDD is up to date.

The reliance on third parties in AML 9.1.1 may not be applied to the cases where the third party is resident in a country with high geographical risk factors.

The relationship between the Relevant Person and the third party should be subject to a contractual agreement.

22. The existence of the consent of the customer to the gathering, processing, storage and provision, including, if necessary, to third parties, of his/her personal data, confirmed by an identification tool is obligatory for the Bank.

23. The Bank, however, retains responsibility for any failure to comply with a requirement of the AIFC AML Rules, as this responsibility cannot be delegated.

Article 7. Information provided to the FIU

24. The Bank provides to the FIU the information on the following transactions:

1) threshold transaction in accordance with the legislation on AML/CFT;

2) suspicious transactions, which there are reasons to believe are aimed at the ML/FT.

25. The criteria and signs of identifying transactions, the content, form and timing of submission of threshold transaction and suspicious transactions are regulated in the regulatory legal acts of the legislation in the area of AML/CFT shall be set forth in the internal normative documents of the Bank.

26. Documents and information on threshold transactions and suspicious transactions, as well as the results of the examination of all complex, unusually major and other unusual transactions are sensitive documents, and should be kept throughout the entire period of business relationships with the customer and at least six years after the transaction.

27. The documents and information shall contain information that makes it possible to restore the Client's transactions, including the amounts and types of currencies.

Article 8. Training and education of employees

28. The Bank conducts AML/CFT training for its employees in accordance with the legislation on AML/CFT in the manner provided for by internal normative documents of the Bank.

29. The purpose of training employees of the Bank is to acquire the AML/CFT knowledge required to comply with the legislation on AML/CFT, internal normative documents on AML/CFT.

30. Training and education include:

1) examination of regulatory legal acts of the legislation in AML/CFT and international AML/CFT standards, as well as the amendments thereto;

2) examination of requirements of the internal normative documents on AML/CFT for the proper performance by employees of the Bank of their official duties, as well as responsibilities for non-fulfillment / improper fulfilment of the requirements of the legislation, internal normative documents on AML/CFT;

3) examination of typologies, schemes and methods of ML/FT, as well as signs of identifying suspicious transactions.

31. If the Bank relies on the third parties to conduct one or more elements of CDD on its behalf, then these third parties undergo AML training.

Article 10. Responsibility

32. Heads of the structural subdivisions of the Bank involved in the AML/CFT process shall be charged with supervising execution of this Policy.

33. Non-fulfillment / improper fulfilment of the Policy is considered as a non-fulfillment / improper fulfilment of the duties by the relevant employees of the structural subdivisions of the Bank, with the possible bringing them to disciplinary or other responsibility in the manner determined by the internal normative documents of the Bank and the legislation.

Article 11. Final provisions

34. The Policy enters into force from the date of approval by the relevant authority, unless another period is stipulated by the decision of the authorised body of the Bank upon its approval.

35. The Policy is revised in case of changes in the requirements of the legislation, international AML/CFT standards and other cases.

36. Issues not directly regulated by the Policy are regulated by the relevant internal normative documents of the Bank, the legislation.

37. If the provisions of this Policy contradict the requirements of the effective legislation, the legislation shall apply.