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	Updated by CCO	13/06/2022	Board of Directors
2.0	Updated by CCO	27/12/2024	Board of Directors

Content

1. The General Provisions

1.1. The Policy on combating the legalization (laundering) of proceeds from crime, financing of terrorism and the financing of proliferation (the "AML Policy") is drafted in accordance with legislation of the Republic of Kazakhstan and the Astana International Financial Centre (AIFC) on AML/CFT/CPF (the “legislation on AML/CFT/CPF”), the Financial Action Task Force (the “FATF”) recommendations, international standards, best international AML/CFT/CPF practice and clarifications of the Astana Financial Services Authority (the “AFSA”) , FIU).

1.2. The purpose of the AML Policy is to create an internal control system in the Brillink Bank (the “Bank”) for AML/CFT/CPF purposes, to prevent the involvement of the Bank and their employees in operations related to the money laundering, the financing of terrorism and the proliferation financing (the “ML/FT/PF”). For these purposes, the Bank has agreed:

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

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

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

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

2. Definitions

2.1. **Beneficial owner**

2.1.1. (1) Beneficial owner, in relation to a customer, is:
(a) for an account – a natural person who ultimately owns, or exercises effective control over the account;
(b) for a transaction – a natural person on whose behalf or for whose benefit the transaction is being conducted;
(c) for a legal person or arrangement – a natural person who ultimately owns or exercises effective control over the legal person or arrangement.
(2) Without limiting subrule (1) (a), a beneficial owner for an account includes any natural person on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are acting (either temporarily or permanently).
(3) Without limiting (1) (c), the beneficial owner for:
(a) a legal person includes:

(i) a natural person who, directly or indirectly, owns or controls at least25% of the shares, participation interest or voting rights of the legal person; or
(ii) a natural person who, directly or indirectly, otherwise exercises control over the legal person's management;
(b) a legal arrangement that administers and distributes funds (such as a trust) includes:
(i) where the beneficiaries and their distributions have already been determined - a natural person who is to receive at least 25% of the funds of the arrangement;
(ii) where the beneficiaries or their distributions have not already been determined – a natural person who is part of the class of natural persons for whose benefit the arrangement is established or operated and who could receive at least 25% of the funds of the arrangement; or
(iii) where a natural person, directly or indirectly, exercises control over at least 25% (by value) of the property of the arrangement.

2.2. **Business relations**

2.2.1. Business relations - relations for the provision by the Bank to the customer of services (products) related to financial activities and financial services.

2.3. **Customer**

2.3.1. Customer - an individual or legal entity (including a sole proprietor and a foreign structure without forming a legal entity) receiving the Bank's services.

According to the Conduct of business Rules the Astana International Financial Centre (the "AIFC") NO. FR0005 OF 2017, the Bank has the following categories of customers: professional customer and market counterparty.

For the purposes of this AML Policy, "foreign structure without forming a legal entity" means foundation, partnership company, trust, company, partnership, organization, or other corporate entity established in accordance with the laws of a foreign state, which are considered as independent organizational and legal forms, regardless of whether they have the status of a legal entity of a foreign state where they are created.

2.4. **Financing of terrorism**

2.4.1 For the purposes of this AML Policy, "financing of terrorism" means the provision or collection of money and (or) other property, the right to property or property benefits, as well as gifts, exchanges, donations, charitable assistance, the provision of information and other types of services or the provision of financial services to an individual or a group of persons , or to a legal entity, committed by a person knowingly aware of the terrorist nature of their activities or that the provided property, provided information, financial and other services will be used to carry out terrorist activities or provide for a terrorist group, terrorist

organization, illegal paramilitary formation.

2.5. **Customer due diligence**

2.5.1 Customer due diligence (the “CDD”) 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/PF.

2.6. **Financial Intelligence Unit of the Republic of Kazakhstan**

2.6.1 For the purposes of this AML Policy, “Financial Intelligence Unit of the Republic of Kazakhstan” (the “FIU”) means an authorized state body that carries out financial monitoring and takes other measures to combat the ML/FT/PF in accordance with the legislation on AML/CFT/CPF.

2.7. **Legalisation (laundering) of proceeds from crime**

2.7.1 For the purposes of this AML Policy, “legalization (laundering) of proceeds from crime” means 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.

2.7.2 Proceeds of crime - money and (or) other property received because of a criminal offense.

2.8 **The money laundering, the financing of terrorism and the proliferation financing**

2.8.1 For the purposes of this AML Policy, “the money laundering, the financing of terrorism and the proliferation financing” (the “ML/FT/PF”) the money laundering, the financing of terrorism and the proliferation financing – the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

2.9 **ML/FT/PF risk management**

2.9.1 For the purposes of this AML Policy, “ML/FT/PF risk management” means a set of measures taken by the Bank to identify, assess, monitor and minimise ML/FT/PF risks, both in relation to the customer and its transactions, and in relation to the Bank’s products/services and processes.

2.9.2 Risks of ML/FT/PF - the possibility of intentional or unintentional involvement of the Bank in ML/FT/PF processes or other criminal activities.

2.10 Money Laundering Reporting Officer

2.10.1 For the purposes of this AML Policy, “Money Laundering Reporting Officer” (the “MLRO”) is a person with responsibility for implementation and oversight of its compliance with the AML Policy, who has an appropriate level of seniority and independence to act in the role.

2.11 Politically Exposed Persons

2.11.1 For the purposes of this AML Policy, “Politically Exposed Persons” (the “PEP”) is a natural person (including a family member or known associate) who is or has been entrusted with a prominent public function, including but not limited to: a head of state or of government, senior politician, member of a legislative or constitutional assembly, senior government official, senior judicial official, senior military officer, ambassador, senior person in an international organisation, senior executive of a state-owned entity, a senior political party official, or an individual who has been entrusted with similar functions such as a director or a deputy director; at an international, national, or regional level.

This definition does not include middle-ranking or more junior individuals in the above categories.

2.12 Sanctions

2.12.1 Sanctions list issued by the Republic of Kazakhstan - persons included in the list of persons involved in terrorist activity and/or in the list of persons and organizations associated with the financing of terrorism and extremism, as well as in the list of persons and organizations associated with the financing of proliferation of weapons of mass destruction, obtained in accordance with the legislation on AML/CFT/CPF.

2.12.2 The relevant resolutions or sanctions issued by the United Nations Security Council (UNSC) - persons or organizations subject to international sanctions in accordance with the resolutions of the UNSC.

2.12.3 Sanctions lists – official documents that contain the names of individuals, groups, and organizations against which economic or legal restrictions are directed, developed by authorized international organizations and states (for example, sanctions issued by the Council of the European Union (EU) , the US Department of the Treasury’s Office of Foreign Assets Control (US) , United Kingdom (HM Treasury) issued by the UK government (UK) ,HK, CN sanctions list and others).

2.12.4 Targeted financial sanctions - measures to freeze transactions with money and (or) other property, taken by the Bank and state bodies in accordance with the legislation on AML/CFT/CPF and resolutions issued by the UNSC related to the prevention and prevention of terrorism and financing of terrorism, and the prevention, obstruction and stop the proliferation of weapons of mass destruction and their financing.

2.12.5 Freeze of transactions with money and (or) other property - measures taken by the Bank to suspend the transfer, transformation, alienation, or

movement of money and (or) other property.

2.12.6 Blacklist - a list of individuals and legal entities that are under the financial monitoring of the Bank. Includes:

a) persons identified as suspicious during the CDD, in the process of monitoring and analysing customers and (or) their transactions;

b) a list of persons received from state bodies for the purpose of monitoring.

2.13 Financial monitoring

2.13.1 For the purposes of this AML Policy, “financial monitoring” means a set of measures for the collection, processing, analysis and use of data and information on transactions with money and (or) other property carried out by the FIU and the Bank in accordance with the legislation on AML/CFT/CPF.

2.13.2 Suspicious transaction with money and (or) other property (“suspicious transaction”)– a transaction of the customer (including an attempt to perform such a transaction, a transaction in progress or a completed transaction), in respect of which there are suspicions that the money and (or) other property used to perform it are proceeds from crime, or the transaction itself is aimed at the ML/TF/PF or other criminal activity.

2.13.3 Transactions subject to financial monitoring (“threshold transaction”) - transactions of a customer of a subject of financial monitoring with money and (or) other property, in respect of which, in accordance with the legislation on AML/CFT/CPF, financial monitoring is established.

2.13.4 Transactions with money and (or) other property - actions of individuals and legal entities with money and (or) other property, regardless of the form and method of their implementation, aimed at establishing, changing, or terminating the civil rights and obligations associated with them.

2.13.5 Unusual operation (transaction) - an operation (transaction), which is subject to compulsory analysis on the grounds specified in paragraph 8.3.6 of the AML Policy.

2.14 Shell bank

2.14.1 For the purposes of this AML Policy, “shell bank” means a non-resident bank that does not have a physical presence in the state (territory) in which it is registered as a bank and (or) received a license to carry out banking activities, with the exception of such a bank being directly or indirectly owned by a banking a holding subject to consolidated supervision in the state (territory) in which it is registered.

3 Organisation of internal control for AML/CFT/CPF purposes

3.1 The Bank appoints an individual as MLRO, with responsibility for implementation and oversight of its compliance with the AML Policy, who has an appropriate level of seniority and independence to act in the role.

3.2 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.

3.3 The Bank also determines the deputy MLRO. In this case, the MLRO performs managerial functions, and the deputy MLRO performs executive functions.

3.4 The functions of the MLRO/deputy MLRO:

a) implementation of the legislation on AML/CFT/CPF and international AML/CFT/CPF standards;

b) organisation of reporting and control over the reporting to the FIU in accordance with the legislation on AML/CFT/CPF and promptly notifies the AFSA of such a submission;

c) other functions established by the legislation on AML/CFT/CPF and internal documents of the Bank.

3.5 Organisation of the internal control system for AML/CFT/CPF 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/PF, where:

a) first line of defence is all employees of the Bank who are responsible for timely reporting to the MLRO/deputy MLRO information about violations, shortcomings, events, transactions that may lead to the risk of ML/FT/PF;

b) second line of defence is MLRO/deputy MLRO and Internal control officer;

c) third line of defence is an internal auditor who independently evaluates the effectiveness of the internal control system for AML/CFT/CPF purposes.

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

a) responsibility for the creation and effective operation of the internal control system for AML/CFT/CPF purposes lies with the Board of Directors of the Bank;

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

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

d) 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/CPF;

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

f) for AML/CFT/CPF 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.

3.7 The internal auditor conducts an independent assessment of the effectiveness of the internal control system, including an assessment of the effectiveness of processes and procedures for managing ML/FT/PF risk. The audit is carried out in accordance with the Bank's annual internal audit plan and the Bank's procedures.

3.8 The Bank has the internal documents on internal control issues for AML/CFT/CPF 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/PF 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 MLRO/deputy MLRO.

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

3.10 The Bank establishes and maintains systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions issued by:

- the FIU;
- the AFSA; and
- the FATF,

concerning the matters:

(a) arrangements for AML/CFT/CPF in a particular country or jurisdiction, including any assessment of material deficiency against relevant countries in adopting international standards; and

(b) the names of persons, groups, organizations or entities or any other body where suspicion of ML/FT/PF exists.

4 Customer Due Diligence

4.1 For CDD the Bank records information about the customer (its representative), the UBO 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 legislation on AML/CFT/CPF on the customer (and/or its representative) and the UBO.

4.2 The Bank chooses between the standard due diligence and the enhanced due diligence, depending on the customer's risk level, in accordance with the legislation on AML/CFT/CPF.

4.3 The Bank, in the process of CDD, screens the customer and his UBO against the PEP list and his members of their families and to their close associates ("affiliated person").

4.4 The Bank uses an automated information system to update the sanctions list issued by the Republic of Kazakhstan, the relevant resolutions or sanctions issued by the UNSC, the sanctions lists and blacklist, and to perform screens on an on-going basis against customer databases and records for any names appearing in resolutions or sanctions issued by the Republic of Kazakhstan, UNSC or by the US, EU, UK, HK, CN and blacklist, as well as to monitor transactions accordingly.

4.5 Information received in the framework of the customer identification (its representative) and the UBO 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.

4.6 The frequency of updating and/or the need to obtain additional information on the Customer (its representative) and the UBO established taking into account the level of risk of the Customer (group of customers) and/or the degree of exposure of the services (products) of the Bank provided to the Customer to ML/FT/PF risks, is carried out in the following order:

a) for a high-risk customer – 1 (one) time per year;
b) for a middle-risk customer - 1 (one) time in 3 (three) years.

4.6 The Bank on an annual basis assesses the degree of exposure of its services and products to ML/FT/PF risks considering the information from the ML/FT/PF risks assessment report and the specific risk category, as well as their minimization. The Bank also takes into account additional information for the period specified in the AML System that affects the final degree of risk:

1) the number of suspicious transactions reports sent by the Bank to the FIU;
2) the number of customer reports on threshold transactions, to be sent by the Bank to the FIU.

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

4.8 Non-face to face establishment of business relations with a customer is carried out by the Bank in the manner and in accordance with the requirements provided for by the legislation on AML/CFT/CPF, the AML Policy and (or) procedures of the Bank.

4.9 The Bank does not establish non-face to face business relations with an individual/legal entity/ a foreign structure without forming a legal entity included in at least the following lists:

a) the sanctions list issued by the Republic of Kazakhstan;

b) UNSC sanctions and resolutions;

c) FATF high-risk jurisdictions list.

4.10 The Bank establishes data protection systems to keep all records relating to CDD, risk assessment, reporting and customer profile in compliance with the requirements of the Law of the Republic of Kazakhstan on personal data protection dated May 21, 2013, and AIFC Data Protections Regulations and Rules.

5 ML/FT/PF risk management

5.1 For the purposes of ML/FT/PF 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/PF risks assessment methodology is developed and the procedure of assigning, timing and grounds for reviewing the level of ML/FT/PF risks, the procedure for recording, accounting ML/FT/PF risks, control measures and procedures for management and mitigation of ML/FT/PF risks and the procedure for verifying the effectiveness of ML/FT/PF risk management program are determined.

5.2 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.

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

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

a. 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);

b. prohibit the opening and maintenance of correspondent accounts with a Shell Bank, or a bank which is known to permit its accounts to be used by Shell Banks;

c. 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;

d. 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;

e. 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;

f. check PEP list and his affiliated person for his/their involvement in the cases of ML/FT/PF when establishing/continuing business relations, conducting transactions (deals);

g. 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/CPF for identification;

h. 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 establish a business relationship;

- not conduct a transaction with or for the customer through a bank account;

- not open an account or otherwise provide a service;

- terminate any existing business relationship with the customer;

- consider whether the inability to conduct or complete CDD

necessitates the making of a suspicious transaction report;

i. approve of internal documents on AML/CFT/CPF and update them in a timely manner in accordance with amendments to the legislation on AML/CFT/CPF;

j. use and improve the automated information system for AML/CFT/CPF purposes;

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

l. 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/PF;

m. train and test the knowledge of employees of the Bank on AML/CFT/CPF;

n. take other actions for AML/CFT/CPF purposes.

6 Monitoring and analysing customer transactions

6.1 For monitoring and analysing customer transactions, the Bank carries out activities aimed at setting goals and grounds for all threshold, unusual, suspicious transactions, and transactions, that have characteristics corresponding to the typologies, schemes and methods of ML/FT, and in case of necessity the source of financing.

6.2 The Bank uses an automated information system to detects threshold unusual, suspicious transactions, and transactions, that have characteristics corresponding to the typologies, schemes and methods of ML/FT from all performed transactions. Automatic detection is carried out based on scenarios and algorithms developed by the MLRO/deputy MLRO in the terms of reference.

6.3 The Bank provides to the FIU the information on the threshold, unusual, suspicious transactions, and transactions, that have characteristics corresponding to the typologies, schemes and methods of ML/FT.

6.4 The criteria and signs of identifying transactions, the content, form and timing of submission of threshold, unusual, suspicious transactions, and transactions, that have characteristics corresponding to the typologies, schemes and methods of ML/FT are regulated in the regulatory legal acts of the legislation in the area of AML/CFT/CPF shall be set forth in the internal documents of the Bank.

6.5 Documents and information on threshold, unusual, suspicious transactions, and transactions, that have characteristics corresponding to the typologies, schemes and methods of ML/FT 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.

7 Training and education of employees

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

7.2 The purpose of training employees of the Bank is to acquire the AML/CFT/CPF knowledge required to comply with the legislation on AML/CFT/CPF, internal documents on AML/CFT/CPF and international standards in AML/CFT/CPF.

7.3 Training and education include:

a. study of the legislation and international standards on AML/CFT/CPF, as well as the amendments there to;

b. studying the internal documents on AML/CFT/CPF for the proper performance by employees of their official duties, as well as responsibilities for non-fulfilment/ improper fulfilment of the requirements of the legislation, internal documents on AML/CFT/CPF;

c. study of typologies, schemes and methods of ML/FT/PF, as well as signs of identifying suspicious transactions.

8 Know your employee (KYE)

8.1 The Bank provides adequate procedures to ensure high standards when hiring employees. The objective of the KYE process is:

a. to provide the Bank with a clear and comprehensive understanding of its workforce, ensuring that the individuals it brings into align with its ethical and operational values;

b. to maintain trust and security in the banking environment; and

c. to comply with the relevant Kazakhstan's regulatory requirements and AIFC standards.

8.2 The verification process of the KYE process involves:

a. personal data verification - confirmation of personal information, education, and employment history.

b. negative background check - checking government databases for the presence of negative, including criminal, information.

c. conflict of interest assessment - questionnaire to identify potential conflicts of interest.

d. interview - conducting interviews to assess fit with corporate culture and professional suitability.

8.3 For key positions such as Director, CFO, CRO, Compliance, in-depth evaluation and detailed consideration of professional and personal history of the applicant are required. In addition, specific requirements from “Regulatory Guidance On Fitness and Propriety” shall be observed in recruiting these key positions and additional information may be requested by the regulator on a case-by-case basis.

9 Responsibility

9.1 The Bank's employees involved in the AML/CFT/CPF process shall be charged with supervising execution of this AML Policy.

9.2 Non-fulfillment / improper fulfilment of the AML Policy is considered as a non- fulfillment / improper fulfilment of the duties by the relevant employees of the Bank, with the possible bringing them to disciplinary or other responsibility in the manner determined by the labour, administrative and criminal legislation of the Republic of Kazakhstan, internal normative documents of the Bank and the legislation.

10 Final provisions

10.1 The AML 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.

10.2 The AML Policy is revised at least once every two years or in case of changes in the requirements of the legislation, international AML/CFT/CPF standards and other cases.

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

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