



ZIRAAT BANK AZƏRBAYCAN ASC

Approved by decision of the Supervisory Board  
dated 05 September 2023 (Protocol No 68)

A handwritten signature in blue ink, appearing to read "Ilker Met", positioned above a horizontal line.

Dr. Ilker Met

The Chairman of the Supervisory Board

---

**“ZIRAAT BANK AZERBAIJAN” OJSC POLICY  
ON ANTI-MONEY LAUNDERING AND COMBATING  
THE FINANCING OF TERRORISM**

---

BAKU – 2023

## Table of contents

1. CONCEPTS AND SUMMARIES .....	1
2. GENERAL PROVISIONS .....	7
3. PURPOSE AND OVERVIEW OF POLICY .....	7
3.1. Duties and Responsibilities .....	8
3.2.1. Supervisory Board .....	8
3.2.2. Executive Board .....	8
3.2.3. Responsible Person .....	9
3.2.4. Internal Audit .....	10
3.2.5. Requirements for Bank employees: .....	11
3.3 Compliance and Disciplinary measures for Bank employees .....	11
4. AML/CFT INTERNAL CONTROL PROGRAM .....	11
5. CUSTOMER DUE DILIGENCE PROGRAM (KNOW YOUR CUSTOMER - KYC) .....	13
6. PROHIBITED BUSINESS RELATIONSHIPS .....	15
7. RISK-BASED APPROACH PRINCIPLES .....	15
7.1 General Risk Assessment .....	16
7.1.1 Customer risk factors: .....	16
7.1.2 Product, service and operational risk factors: .....	16
7.1.3 Delivery channel risk factors: .....	16
7.1.4 Countries and geographic risk factors: .....	17
7.2. Customer Due Diligence measures (CDD-EDD) .....	17
8. REGULATED TRANSACTIONS .....	18
9. BANK INSTITUTIONAL RISK ASSESSMENT .....	19
10. VERIFICATION MEASURES: .....	19
MITIGATING RISKS OF NEW TECHNOLOGIES .....	19
11. COMPLIANCE WITH SANCTIONS, PEP LISTS, AND TARGETED FINANCIAL SANCTIONS .....	20
12. TARGETED FINANCIAL SANCTIONS - ASSET FREEZING .....	21
13. ACCOUNTABILITY .....	22
13.1 Feedback by the FMS .....	23
13.2 Reporting to management .....	23
14. ESTABLISHING CORRESPONDENT BANKING RELATIONSHIPS .....	23
15. DOCUMENT STORAGE AND RETENTION .....	24
16. ANTI - BRIBERY AND CORRUPTION .....	24
'Whistleblow' mechanism: .....	25
17. IMPLEMENTATION AND ENFORCEMENT OF POLICY .....	26

**“ZIRAAT BANK AZERBAIJAN” OJSC POLICY  
ON ANTI-MONEY LAUNDERING AND COMBATING  
THE FINANCING OF TERRORISM**

“Ziraat Bank Azerbaijan” Open Joint Stock Company is part of the esteemed Ziraat Financial Group. We are fully committed to upholding the highest ethical and legal standards in all our operations, in strict adherence to the relevant legislation. Our unwavering focus on anti-money laundering (AML) and counter-terrorism financing (CTF) measures demonstrates our dedication to combating the illegal acquisition and transfer of funds.

**1. CONCEPTS AND SUMMARIES**

<b>Concept abbreviation</b>	<b>Concept definition</b>
AML/CFT	Measures implemented to prevent, detect, and combat the legalization of criminally obtained property and the financing of terrorism, in accordance with applicable laws and regulations.
Criminally obtained funds or other property	Funds of any kind, movable or immovable, tangible or intangible property, legal documents confirming ownership rights, obtained directly or indirectly through the commission of crimes provided by the Criminal Code of the Republic of Azerbaijan.
Legalization of criminally obtained funds or other property	Conversion or transfer of funds or other property for the purpose of concealing the true source of the acquisition of funds or other property, knowing that it was obtained through crime, or helping the offender to evade responsibility, or carrying out financial transactions or other transactions using criminally obtained funds or other property for those purposes, or covering up or concealing the true nature, source, location, disposition, transfer of funds or other property, rights to such funds or other property, or who owns them knowing it was obtained criminally
	Intentional collection or giving of funds or other property knowing that they will be used in whole or in part, directly or indirectly in order to finance preparation, organization and perpetration of actions envisaged in the relevant articles of the Criminal Code of Azerbaijan by a person or a group (gang, organization) or an individual terrorist or a terrorist group (organization, community) regardless of source of their obtaining.

<p>Financing of terrorism</p>	<p>The following crimes are covered by this definition:</p> <ul style="list-style-type: none"> <li>● Attacking individuals or organizations under international protection,</li> <li>● Committing acts of terrorism or providing material support to terrorists,</li> <li>● Inciting others to commit acts of terrorism,</li> <li>● Providing training for the purpose of terrorism,</li> <li>● Taking hostages,</li> <li>● Hijacking air, water, or rail transport vehicles,</li> <li>● Engaging in piracy or maritime violence,</li> <li>● Illegally acquiring or handling radioactive materials,</li> <li>● Threatening to use or extorting radioactive materials,</li> <li>● Attempting to kill a government official or public figure,</li> <li>● Seizing or attempting to seize power through force,</li> <li>● Forming armed groups outside of legal channels,</li> <li>● Armed uprising or insurrections,</li> <li>● Participating in armed conflicts outside of the country's borders.</li> </ul>
<p>Persons designated within the framework of combating the financing of terrorism</p>	<p>Natural and legal persons subject to sanctions and whose list is approved in the manner determined by the relevant executive body based on legislation of the Republic of Azerbaijan and international agreements, which it is a party to, as well as relevant resolutions of the Security Council of the United Nations as part of the fight against the financing of terrorism.</p>
<p>Sanction lists</p>	<p>These are the international lists of designated persons determined by the Sanctions Committees of the United Nations Security Council and a domestic list of designated persons determined by the orders of the courts of the Republic of Azerbaijan on the basis of a submission of the competent executive authority established to suppress and prevent the terrorism and terrorist financing, as well as the proliferation of weapons of mass destruction and its financing</p>

Financing of proliferation of weapons of mass destruction	Act of raising or providing assets, as well as providing financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery (their missiles, rockets and other unmanned systems) and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national law of the Republic of Azerbaijan or its international obligations.
Human trafficking	Recruitment, transportation, transfer, harboring or receipt of persons by means of threat, use of force or other terms of coercion, abduction, fraud, deception, abuse of power or vulnerability, or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation includes prostitution, forced labor, slavery, servitude or the exploitation of others, including children. Even if these methods are not used, the act of receiving, transporting, concealing, giving, or receiving people for the purpose of exploitation is considered human trafficking.
High risk countries	Countries or territories identified by credible sources (mutual evaluation reports, detailed assessment reports or follow-up reports published by international organizations and bodies) as not having adequate AML/CFT systems, providing support for armed separatism, extremism, mercenary, terrorist activities, or that have designated terrorist organizations operating within their country, having significant levels of corruption or other related criminal activity, not requiring disclosure of identification data when conducting financial transactions, and are subject to sanctions, embargos or analogous measures issued by international organizations.
FATF	Financial Action Task Force – the inter-governmental body established in 1989 sets international standards in the field of combating the legalization of criminally obtained property, the financing of terrorism and proliferation of weapons of mass destructions.

Wolfsberg Questionnaire (CBDDQ)	The CBDDQ aims to set an enhanced and reasonable standard for cross-border and/or other higher risk Correspondent Banking Due Diligence, reducing to a minimum any additional data requirements, as per the Wolfsberg definition and current FATF Guidance.
Financial Monitoring Service (FMS)	The Financial Monitoring Service of the Republic of Azerbaijan (FMS) is a body exercising powers in the field of anti-money laundering and combating the financing of terrorism as defined by Law as well as participating in policymaking in this area.
Politically exposed persons	Persons who are or have been entrusted with prominent public functions by any country or by an international organization, (Heads of State or of government, heads of state authorities (bodies), their deputies and members of legislative organ, members of the governing bodies of political parties, judges of supreme and constitutional courts, members of the governing bodies of and persons in decision making positions in courts of auditors or the boards of the central banks, extraordinary and plenipotentiary ambassadors, high-ranking military and special rank officers, members of the management or governing bodies of State-owned enterprises and persons in decision-making positions in such enterprises, directors, deputy directors and members of the board or persons in decision making positions in international organizations)
Close relatives of politically exposed persons	Parents, grandparents, spouses, children, grandchildren, siblings and siblings-in-law, adopters of as well as adoptees taken into custody by politically exposed persons
Close associates of politically exposed persons	Natural persons who have joint beneficial ownership of legal entities or foreign legal arrangements, or any other close business relations, with a politically exposed person; natural persons who have sole beneficial ownership of a legal entity or a foreign legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person; natural persons in whose name the property de facto belonging to a politically exposed person is registered

Responsible person	Responsible person oversees the implementation of internal rules and procedures in Bank related to preventing money laundering and financing terrorism. They exchange information with the financial monitoring service, prepare reports on monitored transactions, and ensure compliance with regulations and ethical standards.
Customer	Any natural or legal person permanently or occasionally using the services of the reporting entities or other persons involved in monitoring that concern the transactions with the funds or other property
Business relationship	Professional relationship which reporting entities and other persons involved in monitoring formed with their customers while conducting their professional activity and is based upon mutual rights and duties of parties and are not of a one-time nature.
Foreign legal entity	A legal entity established in a foreign state or territory, which has the legal capacity to hold property and enter into contracts in its own name. In accordance with relevant legislation, property may be transferred to a foreign legal entity, either with or without the condition that the beneficiary or a group of beneficiaries benefit from the founder (a natural or legal entity), or under the supervision of the foreign legal entity provider within the framework of special purposes, without creating a trust or similar institution with similar characteristics. The founder, manager, guarantor, beneficiary, or group of beneficiaries of a foreign legal entity are the individuals or entities who have the relevant rights and duties arising from the founding document of the foreign legal entity.
Beneficial owner	Natural or legal person who ultimately obtains economic or other benefit from the transactions with funds or other property as well as the real owner of the legal person for the benefit of whose transactions are conducted or a natural person who exercises control over the client and (or) on whose behalf financial transactions or other transactions are carried out, or a natural person who exercises control over a legal entity.
Significant participation share	Direct or indirect ownership of a share that constitutes at least 10 percent of the charter capital of a company, as well as the associated voting rights or the ability to exert significant influence on decision-making within the company based on the contractual agreement.

Authorized individual	Person or entity who has been given the legal authority to act on behalf of another person, organization, or entity in a specific matter or capacity. An authorized representative is typically designated through a legal or formal process, such as power of attorney or appointment letter, and is authorized to make decisions on behalf of the person or the entity they represent.
Risk – based approach	Anti money laundering and combating the financing of terrorism involves the systematic classification of customers' products, delivery channels, and other relevant factors, based on their level of risk, progressing from high-risk to low-risk.
Monitoring	Measures of control carried out by the financial intelligence unit, based on the information on transactions with the funds or other property received from the reporting entities, other persons involved in monitoring, the supervision authorities, or other known sources
Information and documents	Any facts, opinions, knowledge, news or other sort of information, as well as documents in paper or electronic form regarding transactions and business relationships, produced, kept, recorded the result of the activity of Bank irrespective of the date of producing, presentation form and classification. This definition also covers facts, knowledge, news or other sorts of information, as well as documents created, stored, registered in various databases, as well as collected on the internet or other network servers.
Electronic transfers	Movement of funds or money from one account to another through electronic means such as wire transfers, online banking, or mobile payment apps, without the need for physical cash or checks. This is a fast, convenient, and secure way of sending and receiving money between accounts, and it is commonly used for both local and international personal and business transactions.
Virtual asset	A digital representation of a value that digitally traded or transferred and can be used for payment or investment purposes. Digital representation of fiat and foreign currency, shares, and other financial instruments is not considered a virtual asset.
Shell-bank	A bank that has no physical presence (mind and management), in the country in which it is incorporated and licensed and/or which is not affiliated with a regulated financial services group that is subject to effective consolidated supervision.



## **2. GENERAL PROVISIONS**

“Ziraat Bank Azerbaijan” OJSC (hereinafter “Bank”) AML/CFT policy (hereinafter "Policy") regulates the anti-money laundering and combating the financing of terrorism in Bank. This policy has been designated to comply with the legislation of the Republic of Azerbaijan, Wolfsberg principles, FATF recommendations and Basel standards. It also adheres to the Law of the Republic of Azerbaijan on combating the legalization of property obtained through crime and the financing of terrorism (hereinafter "the Law"), as well as financial decisions and regulatory acts adopted by the AR Financial Monitoring Service (hereinafter FMS) and the Central Bank of the Republic of Azerbaijan. Furthermore, this policy has been prepared based on the international agreements signed by the Republic of Azerbaijan and the Ziraat Finance Group Compliance Policy.

Bank conducts its financial activities transparently and in accordance with the legal framework of the Republic of Azerbaijan, as well as adhering to international standards, ensuring full compliance with all applicable regulations and best practices. Bank requires all employees to adhere to ethical standards, including honesty and fairness, as well as to comply with anti-corruption policies and avoid conflicts of behavior.

## **3. PURPOSE AND OVERVIEW OF POLICY**

This Policy is a crucial component of Bank's internal control program on AML/CFT issues, outlining the key principles guiding the conduct of AML/CFT operations, internal rules, procedures and control mechanisms regarding prohibited fields for establishing business relationships, and criminal acquisition of responsible persons on money laundering or terrorism financing, as well as identifying development directions.

The internal control program comprises the following in addition to this policy:

- Internal rules and procedures governing customer due diligence measures and risk assessments related to customer profiles;
- methodology and procedures for ascertaining beneficial owners of clients;
- Internal rules and procedures governing the storage and confidentiality of information and documents
- Internal rules and procedures for outlining the criteria (indicators) for detecting or updating, analyzing suspicious transactions, as well as reporting information and documents to FMS;
- Methodology and procedures for institutional risk assessment;
- Internal rules and procedures for creating and launching new products;
- Standards for evaluation of internal control program by internal audit.

The primary objective of this policy is to provide a comprehensive understanding of Bank's strategic vision and countermeasures aimed at preventing its involvement in ML/FT activities linked to criminal proceeds and precluding the use of Bank as an intermediary in this process. Bank's activity strategy expressly prohibits engaging in any activities linked to ML/FT obtained through criminal means. Bank's primary objective is to safeguard its interests, as well as, uphold the reputation and the trust of its customers by refraining from any involvement in criminally

obtained ML/FT, and by delivering banking services that adhere to professionalism, high ethical standards, quality and innovation. Policy also aims to serve as a guide for employees to detect and prevent instances of illegally acquired ML/FT. Policy upholds the principle that all Bank employees comprehend their responsibilities and receive proper training. To effectively implement the measures outlined in Policy, Bank employs advanced international practices consistent with the country's legislative framework, regulatory norms of supervisory bodies, international financial institutions, and institutional risk assessment principles. Policy applies to all Bank divisions and is implemented in conjunction with other internal procedures.

### **3.1. Duties and Responsibilities**

Bank management ensures that employees' rights and duties regarding AML/CFT are clearly defined in their respective job descriptions, and adopts a specialized approach aligning with each position's instructions. The responsibilities and duties of Bank's supervisory, executive and audit bodies are defined as follows.

#### **3.2.1. Supervisory Board**

The Supervisory Board has implemented a system of measures that requires Bank internal rules, procedures and control mechanisms to be drafted in compliance with the Law and other legal acts in the field of AML/CFT, along with the requirements determined by the supervisory body and FMS. Bank is also required to maintain job descriptions for its management and employees, and implement best practices and principles outlined in Bank's charter:

- Reviewing and approving any updates or modifications made to Bank's policy, internal rules, procedural documents
- Promptly reporting any violations of the requirements outlined in the Laws of the Republic of Azerbaijan "On the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism" and "On targeted Financial Sanctions" to the supervision authorities.
- Establishing and maintaining an effective internal control and risk management system, as well as monitoring its ongoing performance to ensure our operations meet the highest standards of compliance.
- Maintaining a clear protocol for the appointment and dismissal of a responsible person with independent decision-making authority within Bank.
- Ensuring the internal audit department operates correctly and efficiently by establishing effective monitoring and review processes
- Establishing a clear and effective organizational structure for Bank's activities related to money laundering and financing of terrorism

#### **3.2.2. Executive Board**

It is imperative to adhere to the internal regulations, procedures, and control mechanisms approved by the Supervisory Board to prevent Bank from becoming a conduit for financing activities related to proliferation and dissemination of mass destruction weapons, fraud, corruption, and other illicit purposes. The Board of Directors plays a crucial role in ensuring the establishment

of a robust internal control mechanism by ensuring that Bank undertakes the necessary efforts. Specifically the Board of Directors shall carry out the following tasks:

- Guarantee proper implementation of AML/CFT policies, rules, and procedures;
- Conducting comprehensive risk assessment and management to prevent illegal operations, including implementing internal control procedures to prevent ML/TF, financing of proliferation of mass destruction weapons, fraud, and corruption, and ensuring customer due diligence and verification measures are in place during the implementation of new technologies, identification of the beneficial owner and the application of other similar procedures, as well as providing regular supervision during these activities;
- Ensure the implementation of Bank's current policy and other internal control program documents, and deliver to them to employees;
- Verify compliance of Bank's AML/CFT system with legal and internal bank documents.
- Provide the relevant structural unit with appropriate software and adequate human resources to implement AML/CFT measures effectively;
- Provide feedback on the acceptance of new clients and the establishment or termination of business relations with high-risk clients, as needed;
- Carry out necessary work and create the required conditions within Bank to effectively detect and prevent suspicious transactions in a timely manner;
- Review Bank's institutional risk assessment report on AML/CFT, analyze the results, order the implementation of measures to reduce identified risks, approve an action plan for managing residual risks, and ensure relevant employees are familiar with it;
- Take appropriate action against employees who fail to comply with Bank's internal rules and procedures related to AML/CFT, or who create obstacles to their implementation.

### **3.2.3. Responsible Person**

Responsible person is selected from among individuals representing Bank at the management, control, and/or executive levels acting on behalf of the Ban, not performing internal audit or customer service functions. Supervisory Board decides on the appointment or dismissal of this individual and provides the reasons to supervision authorities. Responsible person's duties cannot be influenced by other structural units. Furthermore, individuals engaged in labor activities with another monitoring subject or who have a close familial relationship with members of the monitoring subject's management are not eligible to serve as responsible persons. Responsible person has the authority to make independent decisions on suspicious transactions and to provide instructions to relevant Bank employees and structural units regarding AML/CFT. Responsible person, in collaboration with Bank's employees and structural units, identifies and expeditiously halts any suspicious transactions, in accordance with internal rules, procedures, and control mechanisms, and promptly provides complete and comprehensive information and documents to the FMS.

The department responsible for AML/CFT functions within Bank should solely focus on internal control and AML/CFT activities, with enough personnel to ensure high-quality work. Responsible person, along with any Bank employees involved in AML/CFT, has the right to access any information and documents stipulated by the Law. Responsible person should be involved

early in the planning, development, and implementation of new products and services to proactively identify and mitigate potential risks, particularly in managing money laundering and terrorist financing risks.

Responsible person must meet the following requirements in terms of professional qualifications and experience:

- At least 2 years of work experience in the relevant field of higher education and within the primary scope of the monitoring subject's activity
- Knowledge of national legislation, international standards, and requirements related to anti-money laundering and combating the financing of terrorism
- Familiarity with the key areas of the monitoring subject's operations
- Absence of any criminal convictions.

Responsible person's duties include:

- Monitoring employee compliance with the Law, as well as internal rules, procedures, and control mechanisms, in accordance with the direction of Bank's activities;
- Conducting daily monitoring of bank transactions and supervising the application of continuous customer due diligence measures, preparing relevant reports on current and suspicious transactions, and ensuring they are submitted to the supervision authorities within the prescribed legislative deadlines;
- Responding to requests from the FMS regarding the information and documents on bank transactions conducted in Bank;
- Organizing regular training for employees involved in AML/CFT activities;
- Implementing measures aimed at resolving any issues that may arise due to the termination of transactions;
- Informing management every 6 months about potential risks associated with high-risk transactions, money laundering, and terrorist financing, including risk assessments on customer characteristics, products, services, operations, delivery channels, and geographical locations. Furthermore, providing general statistical information on the reports and suspicious transactions submitted to the FMS.
- Reporting any violations of AML/CFT laws committed by employees to Bank's management;
- Carrying out any other duties stipulated by the relevant legislation in the field of AML/CFT.

#### **3.2.4. Internal Audit**

The Internal audit department of Bank assesses the effectiveness of the application of legal acts and the internal control program related to AML/CFT policies, internal rules, procedures, and control mechanisms. The main objective is to promptly detect potential errors and deficiencies in the application of requirements and to minimize associated risks. The services of Ziraat Bank A.S. or external audit organizations may be used to ensure compliance with international standards. The Audit Committee is responsible for conducting regular audits to verify compliance with

requirements. The frequency and duration of audit inspections should be at least once a year, based on the risk level of the inspected area. Inspection results must be prepared no later than 5 working days after the audit's completion and formalized with an auditor's opinion reflecting objectives, scope, and audit results, as well as a report on identified defects and deficiencies, and recommendations for each problematic area. The final report should be submitted to Bank's management information and to the Audit Committee for control purposes.

#### **3.2.5. Requirements for Bank employees:**

- Understand and comply with the current Policy and related normative documents;
- Implement measures outlined in Policy and relevant normative documents;
- Inform Responsible person and the relevant structural unit responsible for AML/CFT of high risk and unusual cases defined in the AML/CFT legislation;
- Promptly report information regarding suspicious customers, activities, and transactions to the responsible structural unit and follow the instructions of Responsible person;
- Refrain from disclosing suspicious cases to the client;
- Be aware of the responsibilities and consequences of noncompliance with the requirements arising from the current Policy.

### **3.3 Compliance and Disciplinary measures for Bank employees**

All Bank employees are required to comply with this Policy and other operating procedures regarding AML/CFT. Any violations of this Policy or AML/CFT procedures may result in disciplinary action, such as cancellation of declared bonuses, reprimand, severe reprimand, termination of employment and legal proceedings in accordance with applicable law. Bank also maintains a strict policy against employing any person previously known to be involved in money laundering or terrorist financing.

## **4. AML/CFT INTERNAL CONTROL PROGRAM**

AML/CFT internal control program primary objective is to establish an efficient control mechanism and procedure that effectively regulates activities related to the acquisition, management, and disposition of criminally obtained assets, with the aim of preventing money laundering and terrorist financing.

Bank has implemented a comprehensive internal control program for AML/CFT measures, consisting of the following elements:

- A clear defined policy that reflects Bank's strategy, goals, and principles for combating money laundering and terrorist financing. This policy implements internal rules, procedures, and relevant measures for AML/CFT compliance and established a relevant structural unit responsible for information exchange with the FMS;
- Appointment of a responsible person to oversee legal compliance and implementation of AML/CFT processes within Bank;

- Rigorous verification procedures are applied during the recruitment process to ensure high levels of professionalism and civil integrity;
- Bank provides regular specialized training to employees who have direct customer contact and are authorized to approve transactions, outlining AML/CFT policy, internal rules, procedures, and suspicion indicators, as well as providing detailed guidance on necessary actions;
- An independent audit mechanism, following internal audit standards, is established to evaluate the effectiveness of the existing system.

Bank prohibits the appointment of individuals to management positions who do not meet the requirements of civil integrity. The department responsible for recruitment must verify the civil integrity status of each candidate:

- Individuals convicted of intentional crimes related to property or economic activities, as well as serious or particularly serious intentional crimes
- Individuals legally barred from holding a specific position in the economic sector or engaging in certain activities for a designated period of time.

Bank places a high priority on the professional development of its employees, and to achieve this, it develops and implements a comprehensive training strategy and conducts training sessions accordingly. Bank's training strategy is formulated for the upcoming year during the final month of each year and approved by the Chairman of the Executive Board. AML/CFT trainings are divided into 2 categories: systematic and extracurricular. Systematic training is conducted in accordance with Bank's annual training strategy. The training program can be revised during the year if deemed necessary. These trainings are conducted at least once a year by the structural unit responsible for AML/CFT, as outlined in the program. Quality criteria are strictly followed during the training, and the involvement of third-party experts may be considered to ensure the effectiveness of the program.

Extracurricular trainings are offered under the following circumstances:

- In case of changes in legislative acts or the adoption of new normative documents;
- When there are changes or innovations in Bank's internal policies, rules or procedures;
- If, according to the results of internal audits, Bank is determined to have a high risk of money laundering or terrorism financing occurring due to weak control measures;
- If best practices in international practice require new procedures, rules, or control mechanisms;
- Other justified requests made by Responsible person.

Bank ensures the proper record-keeping by storing training registration data for at least 5 years, including the following information:

- AML/CFT training sessions dates;
- Training purpose and content;
- A sign-in sheet of employees participated in the training.

The Internal Audit department is responsible for ensuring the effectiveness and adequacy of Bank's internal control system for AML/CFT and prepares a report that includes recommendations and suggestions for detecting errors and omissions in the implementation of the related rules and procedures. The report also highlights any weaknesses in the internal control system and provides solutions to address them. The Audit Committee and the Supervisory Board review and discuss these reports to ensure compliance with AML/CFT regulations. Based on the identified deficiencies, an action plan is developed to address the issues, and Bank promptly implements this plan to improve the internal control system and maintain compliance with regulatory requirements.

## **5. CUSTOMER DUE DILIGENCE PROGRAM (KNOW YOUR CUSTOMER - KYC)**

Active personal involvement is crucial in the process of establishing initial business relations with clients, wherein individuals are required to personally participate. The account opening documents are formalized in accordance with the legal requirements, when applying to open a bank account remotely. The documentation must comply with legal requirements, and subsequent account opening and transactions can be performed by authorized representatives or power of attorney, provided that they follow relevant legislation. However, non-resident legal entities and customers cannot open remote bank accounts through authorized representatives. Remote bank accounts can only be opened if Bank obtains all required documentation from state information systems as stipulated by law.

Bank is committed to accurately identifying all of its customers and requires a thorough customer and beneficial owner identification procedure in accordance with Know Your Customer program to establish business relations. Both customer and beneficial owner identification must comply with the requirements outlined in banking legislation.

Bank applies various elements of the Know Your Customer Program in accordance with AML/CFT measures to identify customers, beneficial owners, persons with a significant participation share, and their authorized representatives. The following elements are used within the framework of customer due diligence measures:

- Customer onboarding process
- Identification-verification procedures
- Account monitoring
- Risk-based customer segmentation
- High-risk client monitoring

Bank is required to implement customer due diligence measures in the following instances:

- Prior to establishing business relations
- For any one-time transaction expected to be performed at or above statutory amount
- In case of conducting one-time electronic transfers of financial funds or one-time transactions with virtual assets in accordance with legislation on electronic transfers of financial funds and transactions with virtual assets

- Whenever property is suspected of being acquired through money laundering or used to finance terrorism
- In situations where concerns arise about the accuracy or relevance of information and documents obtained about the client, beneficial owner, persons with a significant participation share, and their authorized representatives.

Bank implements following procedures in conformity with customer due diligence measures:

- Bank must identify the customer, verify their identification information based on reliable and independent sources, and implement other customer due diligence measures where required by law;
- Bank determines whether a person has legal authority to act on behalf of a client or another person, identifies that person, verifies their identification information based on reliable and independent sources, and implements other client due diligence measures;
- Bank identifies the beneficial owner and takes reasonable steps to verify their identification information based on reliable and independent sources;
- Bank explains the purpose and nature of business relationship and obtains necessary information and documents from the client;
- Bank creates a customer profile based on collected data and documents.

Bank strictly adheres to regulatory requirements and legislation when opening accounts for customers. Electronic customer database is entered or updated with customer information during the establishment of business relations, it must be checked and approved by a supervisor or at least one other authorized individual in addition to the operative who conducted the transaction to ensure the accuracy and completeness of data.

Bank consistently applies the following customer due diligence measures:

- Analyzing transactions to assess their compliance with the client's information and documents, as well as their activity and risk profile, including the source of financial sources;
- Reviewing and researching existing information and documents, prioritizing high-risk clients to ensure the adequacy and updating of information within the framework of customer due diligence measures.

Regular monitoring of accounts is implemented by Bank to detect unusual or suspicious signs. Reports of such signs are compiled and reported to Bank management and FMS. Bank continuously implements a risk management process to identify, assess, and mitigate risks related to Know Your Customer program. Bank manages risks associated with the legalization of property obtained through money laundering and terrorism financing by providing protection levels for operational, image, and other risks. Bank has implemented a four-tiered defense system to mitigate the risks of money laundering and terrorist financing:

- **First level** - structural units responsible for customer service and transaction execution
- **Second level** – structural units performing compliance and risk management functions
- **Third level** - Internal Audit department



- **Fourth level** – Ziraat Bank A.S. auditors or external audit.

Each level of defense is responsible for identifying, assessing, and mitigating risks related to money laundering and terrorist financing. The individuals involved in each level work collaboratively and take collective responsibility to ensure effective risk management. Bank aims to enhance its overall compliance framework and protect against financial crime through a coordinated approach.

## **6. PROHIBITED BUSINESS RELATIONSHIPS**

Bank strictly prohibits certain business practices, including opening bank accounts or the documents or property acceptance (in special rooms or safe boxes) under fictitious or anonymous names, as well as the establishment of business relations with shell banks or unidentifiable clients, issuing anonymous deposit certificates and presenting anonymous bank books. Any transaction where the customer identity cannot be determined is strictly prohibited to maintain transparency and prevent fraudulent activities.

Establishing business relations with clients engaged in the following types of activities is strictly prohibited:

- Production, acquisition, development, improvement, or import of nuclear, chemical, bacteriological (biological), and toxin weapons, as well as their means of delivery and related materials (including technologies used for illegal purposes and dual-purpose goods), persons who carry out export, transit transportation, transfer, collection or use, as well as ownership of these weapons or mediation (broker) activities in their international transportation, and provision of financial services;
- Individuals whose names are on local and international lists that require verification as per our policy;
- Persons engaged in the production, sale, or transportation of marijuana, narcotics, and other psychotropic substances;
- Persons involved in red light business or adult entertainment;
- Persons engaged in human trafficking;
- Shell banks;
- Unregulated charities;
- Persons involved in unregulated casino, betting, and gambling;
- Residents of countries that threaten the territorial integrity of the Republic of Azerbaijan (or whose main activity is in this country) or natural and legal persons having business relations with these persons (except international organizations).

## **7. RISK-BASED APPROACH PRINCIPLES**

Bank adheres to the principles of Risk-Based Approach, as recommended by FATF, in its internal control program and AML/CFT risk management process. This approach involves the identification, evaluation, and management of risk associated with customer, transactions, products, counterparties, and countries.

Bank has established risk groups based on the Risk-Based Approach principles to facilitate a thorough assessment of these risks. The customer risk rating is not fixed, but varies based on the customer profile, the purchased product, and the type of transactions they conduct. Customer risk is reevaluated over time, as their business relationship progresses and if there are any changes to their business relationship or operations.

## **7.1 General Risk Assessment**

Bank applies a general risk assessment process when establishing new business relationships or monitoring existing customer relations. This process determines the risk rating for AML/CFT related to the client based on various factors, including:

- Customer type (individuals, entrepreneurs, legal entities);
- Country of origin;
- Countries or territories where it operates;
- Economic activity area;
- Analysis of the beneficial owner, significant shareholder, founder, member of governing bodies, or authorized signatories.

Bank updates the client risk rating in ongoing business relations to ensure it remains accurate and up-to-date by considering the following criteria:

- Customer risk factors;
- Product, service, and operational risk factors;
- Delivery channel risk factors;
- Countries and geographic risk factors.

### **7.1.1 Customer risk factors:**

- The business or professional activities of the customer and its beneficial owners,
- Reputation of customer and its beneficial owner,
- The nature and behavior of the customer and the its beneficial owner,
- Customer with complex ownership structures,
- Companies with bearer shares.

### **7.1.2 Product, service and operational risk factors:**

- Transparency level of the product, service, or transaction,
- Complexity of the product, service, or operation
- Value or volume of the product, service or transaction.

### **7.1.3 Delivery channel risk factors:**

- Direct cash transactions;
- Payment terminals;
- Fast money transfer systems;
- Internet and mobile application;

- Virtual asset or virtual wallet accounts.

Bank acting as either the issuing virtual asset service provider or the beneficiary virtual asset provider, applies customer due diligence measures prior to virtual asset transactions in accordance with legal requirements and verifies the completeness of information provided below to ensure regulatory compliance:

- The virtual asset owner name, including their full name, such as first name, surname, and patronymic for individuals, as well as name, organizational legal form and tax identification number (TIN) for legal entities;
- Virtual asset owner personal identification data, including their birth date and place, personal identification number, and address or national identification number;
- The virtual asset account number or virtual asset wallet address;
- Unique transaction reference number;
- Beneficiary name, including name, surname and patronymic for individuals, as well as name, organizational legal form and tax identification number (TIN) for legal entities
- Beneficiary virtual asset account number or virtual asset wallet address.

#### **7.1.4 Countries and geographic risk factors:**

Bank may apply restrictions and special requirements in accordance with calls made by the Financial Action Task Force (FATF) and high-risk zones designated by Law. Specifically, enhanced customer due diligence measures must be implemented when conducting business dealings and transactions with individuals from high-risk zones, or with individuals who are registered, reside or have a principle place of business in those zones, or with persons holding bank accounts registered in those zones.

Bank is required to implement the measures specified by the FATF in response to their calls.

Following countries and territories are considered high-risk by Bank, in addition to the countries identified by FATF:

- Countries and territories with inadequate AML/CFT systems;
- Countries and territories subject to sanctions or embargoes;
- Countries and territories financing or supporting terrorism;
- Countries and territories with high corruption levels.

#### **7.2. Customer Due Diligence measures (CDD-EDD)**

Bank applies a risk-based approach to customer due diligence measures, ensuring full regulatory compliance before establishing or maintaining any business relationship. In the case of non-compliance, the existing relationship should be terminated and no future transactions should be conducted.

Bank implements the following customer due diligence measures:

- Simplified Due Diligence – SDD
- Standard Due Diligence-STDD
- Enhanced Due Diligence – EDD

Bank follows a risk-based approach in terms of document and information updating, as listed below:

- High risk clients: at least once a year;
- Medium risk clients: at least once every two years;
- Low-risk clients: at least once every three years;
- Politically exposed persons continuously.

The above-mentioned periods may be adjusted based on the outcome of country, sectorial, and institutional risk assessments, as well as other risk factors. Intermediate risk categories and corresponding periods may also be established.

## **8. REGULATED TRANSACTIONS**

Bank conducts mandatory monitoring of transactions in accordance with relevant legislation and regulatory requirements and ensures information transfer to FMS, as necessary.

The detection and analysis of suspicious transactions, as well as, submitting information and documents to FMS, is governed by specific procedural documents that outline the following:

- A process for utilizing indicators or criteria to identify suspicious transactions,
- Method for analyzing the transactions using the criteria or indicators for detecting suspicious transactions,
- Procedures for analyzing transactions that do not meet the criteria or indicator for suspicion,
- Enhanced and continuous customer due diligence measures for suspicious customer profiles and transactions, conducting comprehensive investigations to obtain information and documentation on the source of property,
- Flexible measure to be taken when a transaction is deemed suspicious,
- Procedures for executing FMS requests for information and documents on transactions,
- Analysis of suspicious transactions, as well as the rights duties, and relationship of related parties regarding the submission of information and documents to FMS.

Bank employees must inform Responsible person and provide them with information and documents about the client as a result of monitoring, detailing whether the transaction meets the criteria (indicator) or displays characteristics of money laundering or terrorist financing. Responsible person must then review the information, including additional details on the customer and their activities, and submit it to FMS and Bank management.

Bank continuously monitors customer transactions to ensure they align with the customer profile and business relationship in accordance with AML/CFT program. Front office staff are responsible for regularly updating customer identification information, including beneficial

owners, and taking into account any relevant events occurring during the course of business relations, such as media reports.

The direct supervisor should also be notified when they report a suspicious transaction or activity to Responsible person. The supervisor cannot hold the employee responsible for reporting information about a suspicious transaction to Responsible person. In case of such cases, the employee can report the matter directly to Responsible person without informing their supervisor. The relevant process is carried out under the guidance of safe harbor rules.

Employees who report suspected or actual criminal activity are protected from any criminal or civil liability under international law, even if they are uncertain about the nature of the activity reported or whether it is indeed illegal. This protection promotes transparency and accountability and encourages whistleblowers to come forward.

## **9. BANK INSTITUTIONAL RISK ASSESSMENT**

Bank conducts institutional risk assessment at least once a year to mitigate the risks of money laundering, terrorist financing, and the proliferation of mass destruction weapons. The assessment identifies vulnerabilities and threats faced by Bank and establishes risk criteria, with methodologies and procedures approved by the chairman of Executive Board.

Bank must evaluate the risks associated with potential legalization of property obtained through money laundering or terrorist financing before introducing and launching a new product or service. The product or service information and risk assessment results can be submitted to the FMS for feedback before launching. Executive Board should take appropriate measures to mitigate high-risk products or services.

The institutional risk assessment process is crucial for ensuring that Bank institutional risk management framework aligns with regulatory requirements and international standards. Bank may refuse to provide the product or service, if the risk cannot be reduced or the number of suspicious transactions is too high.

## **10. VERIFICATION MEASURES:**

### **MITIGATING RISKS OF NEW TECHNOLOGIES**

Bank considers business relations and operations involving new and developing technologies as high-risk and takes adequate measures to assess and mitigate the risks of money laundering and terrorist financing during the establishment and implementation of these relationships and operations. Bank management should ensure that appropriate measures are in place for their secure implementation and establish a risk assessment mechanism, prior to introducing new technologies. Bank must develop internal rules and procedures regulating business relationships, products, and transactions created through new technologies or involving their application, and define preventive measures, including the establishment of electronic control systems.

Implementation of new technologies in Bank does not exclude customer due diligence measures. Electronic availability of information and documents is required when customer due diligence measures are implemented through information technology. Utilization of advanced technologies should be declined, if doubts or inconsistencies arise during the identification of the customer and beneficial owner, or if the authenticity of information and documents cannot be verified. Bank employs one or more of the following measures, depending on the type and nature of the transaction to effectively verify documents and the identity of customers during business relationships and transactions conducted without direct communication:

- Confirmation of the customer application using an enhanced electronic signature;
- Verify the information provided by the customer from electronic databases and/or independent external sources
- Perform enhanced customer authentication that require the customer or authorized individual should know (password, PINs, security questions, etc.), possess (mobile application, OTP, TOTP, electronic signature, token, etc.) or are specific to them (face recognition, voice recognition, fingerprint, etc.), meaning these authentication methods (honest identification of a person) employ at least two independent elements to prevent security breaches. Elements independence means that the seizure of one element does not affect the security of other elements;
- Obtain the documents provided by the client from a reliable third party or government agency with the customer consent;
- Conduct correspondence and document exchange through the customer official registered address;
- Require the customer to use security codes, electronic signatures, tokens, and other passwords of this type that confirm their identity when opening their account or virtual office, sent to a verified address by mail, telephone, or other reliable means;
- Verify the customer identity in real-time by video call or video recording over the system.

Customer is required to undergo the 1st, 2nd, 3rd. And 7th verification measures listed above, if a client is conducting business with Bank for the first time. Remote transactions are prohibited, when the identification and verification measures applied during transactions conducted remotely through existing or technologies fail to identify the customer, or if doubts or inconsistencies remain regarding their identity or the authenticity of submitted documents. Customers are not allowed to conduct business through authorized representatives (except for the legal representative of a legal entity) or with non-resident legal entities.

## **11. COMPLIANCE WITH SANCTIONS, PEP LISTS, AND TARGETED FINANCIAL SANCTIONS**

Executive Board of Bank is responsible for ensuring compliance with international standards and best practices regarding sanctions lists and targeted financial sanctions. Bank maintains a database of its customers, beneficial owners, persons with significant participation shares, and

their authorized representatives, in its information system. Bank checks the names of these parties against relevant sanctions lists in the following scenarios:

- Upon the establishment of a business relationship;
- In the event of modifications to customer information;
- In the occurrence of updates to the general sanctions lists;
- In the course of operations not requiring opening of an account.

Bank has implemented an automated verification mechanism in the Bank Information System (BIS) to ensure the matching of customer details, beneficial owners, persons with significant participation shares, and authorized representatives with relevant lists, provided sourced both from FMS and international sources such as Dow Jones Factiva and Refinitiv. Bank conducts daily monitoring of clients and their related parties utilizing these lists, and the BIS sends automatic warnings to the relevant structural department responsible for AML/CFT compliance when names on the lists coincide. Each warning is assessed depending on its status, and decisions are documented and logged in the BIS.

Politically exposed persons (PEPs) are identified through cross-checking with internal and external sources, and by providing the customer with an application/questionnaire form to customer during the account opening process. Establishing business relationships with the customer, whose beneficial owner, persons with a significant participation share, or authorized representatives are classified as PEPs, close relatives of PEPs, or persons with close relations to PEPs, is considered high-risk by the bank system, requiring approval from management and AML/CFT compliance through the relevant structural unit. Transactions involving PEPs, their close relatives, or associates are subject to continuous enhanced due diligence to ensure adherence to AML/CFT regulations.

Bank conducts rigorous screening on various sanctions lists, including but not limited to:

- Domestic monitoring lists determined by the Financial Monitoring Service of the Republic of Azerbaijan;
- Relevant UN sanctions lists;
- Sanctions lists to relevant countries required within the scope of correspondent account activity;
- Politically exposed persons lists;
- Lists required under Ziraat Bankası A.S. AML/CFT policy.

## **12. TARGETED FINANCIAL SANCTIONS - ASSET FREEZING**

Bank is subject to targeted financial sanctions regulations aimed at preventing terrorism, terrorist financing, proliferation of mass destruction weapons, and proliferation financing, as per relevant United Nations Security Council resolutions.

Targeted financial sanctions are intended to supplement rather than replace existing criminal proceedings and primarily rely on following preventive measures:

- Immediate asset freeze,
- Prohibition of asset provision, including providing economic resources, financial services, or assets to sanctioned individuals and entities.

The asset freeze is a critical component of targeted financial sanctions designed to prevent terrorism, terrorist financing, proliferation of mass destruction weapons and proliferation financing. The following assets, irrespective of their direct connection to such activities, must be frozen:

- Assets of sanctioned individuals and institutions;
- Indirectly owned or controlled assets: assets that are owned or controlled directly or indirectly, either alone or with others, as well as any other assets derived from such assets;
- Assets of sanctioned individuals and institutions' representatives: assets of individuals and institutions acting on behalf of or representing sanctioned individuals and institutions;
- Assets of sanctioned entities: assets of entities owned or controlled directly or indirectly, either alone or jointly with others, by the individuals and entities subject to sanctions.

Bank is obligated to freeze intended assets from the moment the international and domestic lists of targeted financial sanctions are published on internet information resources, without delay or prior warning to the parties specified in the relevant article.

Bank must promptly notify FMS of this action and the assets must be held frozen while the individuals and entities subject to sanctions remain on the relevant list and released immediately upon removal from the list.

Individuals and institutions subject to sanctions in banking activities, as well as institutions owned or controlled, directly or indirectly, alone or in partnership with others, and individuals acting on behalf of or representing such individuals and institutions, shall not be provided with assets, economic resources, financial or other related services, either directly or indirectly, alone or in partnership with others.

### **13. ACCOUNTABILITY**

Bank's AML/CFT unit is responsible for submitting reports required by relevant legislation. Transactions exhibiting inexplicable behavior, are not in line with the customer's normal business activity, or lack a typical, rational economic basis are often considered unusual. AML/CFT department should thoroughly investigate such transactions, prepare analysis reports, and provide operational information and documents to the FMS, in accordance with legal requirements.

Information concerning suspicious persons or transactions must be submitted to the FMS through a secure gateway on the designated platform, which Bank is registered and identified on. Only individuals authorized by the chairman of Executive Board may access and receive/ transmit information through this platform. A suspicious transaction is only reported to the FMS with the approval of Responsible person or their substitute.



Responsible person supervises requests related to ML/TF made by the competent state bodies and ensures the timely execution in accordance with legal provisions. Information submitted to the FMS is confidential and may only be accessed by authorized state authorities in compliance with legal requirements. Access to this information is restricted to bank employees who require it in order to carry out their duties and prevent unauthorized disclosure.

### **13.1 Feedback by the FMS**

FMS implements feedback activities to monitor and assess the efficacy of measures undertaken regarding the information and documents submitted to FMS, quality control, and statistical data collection, in strict adherence to legal provisions. The overarching aim of this feedback process is as follows:

- Optimizing the quality of information and documents submitted to FMS by identifying, summarizing, and advising banks on inconsistencies in transactions to be monitored and submitted to FMS;
- Enhancing the effectiveness of transaction analysis by banks,
- Reinforcing the adoption of risk-based approaches towards Bank's clients,
- Strengthening Bank's oversight of operations to be monitored,
- Fostering collaboration between FMS and Bank in combatting ML and FT.

Bank management shall be duly informed of the results of the feedback process at least once every six months, in compliance with established reporting guidelines.

### **13.2 Reporting to management**

Responsible person of Bank shall submit a monthly report to the Compliance Unit of the Parent Bank and a quarterly report to the chairman of the Executive Board containing the following comprehensive information:

- Bank's high-risk customer statistics,
- Corresponding innovations and changes in domestic AML/CFT acts and regulations,
- Statistical information on reports submitted to authorized institutions,
- Analyzed and rejected transaction statistics,
- Requests sent from authorized bodies
- Changes in Bank's Compliance staff
- Organized training for compliance staff
- AML/CFT trainings organized for Bank employees
- Number of new accounts opened and RMA contacts for the correspondent bank

## **14. ESTABLISHING CORRESPONDENT BANKING RELATIONSHIPS**

Correspondent banking relationships involve the execution of financial transactions on behalf of clients of another bank, thereby exposing banks to risks related to money laundering and terrorist financing. In order to mitigate these risks, resident and non-resident banks that seek to establish correspondent relations are subject to a thorough investigation as part of the AML/CFT process by

the responsible structural unit. The relationship pursued only if the investigation yields satisfactory results.

Wolfsberg Questionnaire as part of the investigation, is administered to obtain pertinent information about the correspondent bank's experience with AML/CFT, adequacy of their internal control system for risk assessment, and their business model. Furthermore, documents are obtained and scrutinized to evaluate the correspondent bank's compliance with regulations, banking activity license, share distribution, beneficial owner, management, and internal control systems employed to combat ML/FT and other criminal activities.

Establishing a business relationship with a correspondent bank and opening accounts is only permitted with the approval of bank management. The information provided by correspondent banks is reviewed annually and updated as needed, and new information can be obtained from the correspondent bank if necessary.

Publicly available sources of information are also utilized to evaluate the business reputation of the correspondent bank. The responsibilities and duties of each party are formalized in a comprehensive agreement that accurately reflects their respective roles. It is of utmost importance to emphasize that Bank unequivocally disavows any association with shell-banks and, as such, does not engage in any correspondent banking relationships or banking operations with these entities.

## **15. DOCUMENT STORAGE AND RETENTION**

Bank's Board of Directors is responsible for ensuring that all documents are properly stored for the minimum periods specified below, unless a longer period is mandated by law:

- Domestic and cross-border transaction information and documents must be retained for a minimum of 5 years from the date of the transaction's conclusion, unless the law requires a longer retention period;
- Information and documents obtained, related to business correspondence, account information, and the results of any analysis conducted during customer due diligence measures, must be retained for at least 5 years after the termination of business relations or the end of any one-time transaction, unless a longer period is provided by the legislation.
- Documents and information on unusual transactions, including the results of an analysis conducted to clarify the purpose and nature of these transactions, must be retained for at least 5 years after the termination of legal relations with the client.

## **16. ANTI - BRIBERY AND CORRUPTION**

Bank strictly prohibits any form of corruption or bribery within the framework of its banking activities. It considers any abuse of official power or demand for material or other benefit, privileges or concessions for personal or third-party gain to be unacceptable, and takes adequate measures to prevent such occurrences.

Bank employees are strictly prohibited from accepting gifts that may affect the impartial performance of their duties or create the impression of such influence. Gifts given as a reward for the performance of official duties or creating such an impression are also not allowed. If an employee is unsure whether they should accept a gift or simple hospitality, they should seek the opinion of their direct supervisor. Officials are prohibited from seeking any concessions or privileges in connection with their official activities while concluding or executing civil-legal contracts with natural and legal persons.

If bank employees are offered illegal material or other benefits, privileges or concessions, they should refuse. In cases, where an employee is given such benefits beyond their control, they must inform their direct supervisor and hand over the benefits as required by law.

Any corruption-related offenses committed by bank employees will lead to disciplinary, civil-legal, administrative, or criminal liability, as determined by the legislation. Employees who violate these standards will be held accountable in accordance with the relevant legislation of the Republic of Azerbaijan.

Scope of the Anti-Corruption and Bribery measures:

- All Bank employees, including Supervisory Board;
- Third-party companies and their employees who provide other support services, including services regulated by law;
- Persons and entities providing services on behalf of Bank, including suppliers, consultants, lawyers, and external auditors.

**‘Whistleblow’ mechanism:**

Whistleblow mechanism has been established to allow employees to report any illegal activities, ethical violations or concerns through Bank’s communication channels, such as Skype for Business or [zbazdnk@ziraatbank.az](mailto:zbazdnk@ziraatbank.az) group e-mail to responsible person. Following issues should be reported:

- Fraud,
- Bribery,
- Corruption,
- Forgery,
- Unethical behavior,
- Circumstances creating a conflict of interest,
- Failure to comply with legal regulations.

Whistleblowers are protected from retaliation, including termination, demotion, or any other form of punishment, psychological violence, and pressure or mobbing.

## **17. IMPLEMENTATION AND ENFORCEMENT OF POLICY**

Effective implementation of this policy is the responsibility of Bank's management and employees, who are expected to adhere to its provisions in accordance with the laws of the Republic of Azerbaijan. Policy undergoes annual review during a Supervisory Board meeting to ensure its relevance and effectiveness.

Policy outlined in this document shall take effect on the date of its approval and may only be amended by the Supervisory Board of Bank.

**Agreed:**

Dr. Selchuk Demir  
Chief Executive Officer



Rovshan Ibrahimov  
Member of the Executive Board



Vugar Alipashayev  
Member of the Executive Board



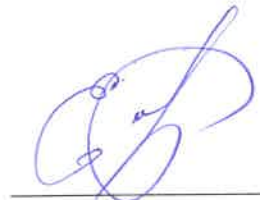
Ahmet Kudret Ishler  
Member of the Executive Board



Seymur Aliyev  
Member of the Executive Board



Tahmasib Eyvazov  
Head of the Legal and Credit  
Risk Liquidation department



Zakariyya Mustafayev  
Head of the Internal Control and  
Compliance department

