TÜRKİYE İHRACAT KREDİ BANKASI A.Ş.

Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing Policy

MAY 2024, İSTANBUL

Document Name	Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing Policy
Document No	POL_AML_05
Version No	V1.4
Issued By	Regulatory Compliance Department

Revision History

Version No	Date	Prepared By	Responsible Department
V1.0	12.10.2006	Internal Control Department	Teoman ŞENER
V1.1	24.11.2016	Regulatory Compliance Department	Regulatory Compliance Department
V1.2	25.12.2020	Regulatory Compliance Department	Regulatory Compliance Department
V1.3	27.12.2021	Regulatory Compliance Department	Regulatory Compliance Department
V1.4	20.05.2024	Regulatory Compliance Department	Regulatory Compliance Department

Revision Details

Version No	Revision Details
V1.0	First Release
V1.1	Reflection of Changes in National and International Legislation
V1.2	Reflection of Changes in National and International Legislation
V1.3	Reflection of Changes in National and International Legislation
V1.4	Reflection of Changes in National and International Legislation and the Bank’s Approach

Document Structure

Related Principal Document	-

Distribution and Announcement

Distribution	All Bank Units
Announcement	All Bank Units

Approval Information

Date	07.06.2024

CONTENTS

1. INTRODUCTION

(1) The Financial Action Task Force (FATF), established to combat the laundering of criminal proceeds, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction on an international scale, requires member countries to comply with its regulations and principles. The Financial Crimes Investigation Board (MASAK), operating under the Ministry of Treasury and Finance of the Republic of Turkey, ensures that Turkey, as a FATF member, adheres to international regulations and enacts necessary legal arrangements in this context.

(2) Türkiye İhracat Kredi Bankası A.Ş., holding a reputable and reliable position internationally, views the fight against money laundering, terrorism financing, and the proliferation of weapons of mass destruction not only as compliance with legal regulations but also as a social responsibility. The Bank places significant importance on this effort, considering it a crucial element of alignment with the international system.

2. LEGAL FRAMEWORK

(1) The Law on Prevention of Laundering Proceeds of Crime No. 5549, Law on the Prevention of Financing of Terrorism No. 6415, and Law on the Prevention of Financing of Weapons of Mass Destruction No. 7262, along with related regulations and communiqués, form the legal basis of the Policy on the Prevention of Laundering Proceeds of Crime, Financing of Terrorism and the Proliferation of Weapons of Mass Destruction.

(2) The Bank also considers the recommendations and standards set by the Financial Action Task Force (FATF), established within the OECD and of which Turkey has been a member since 1991. These standards are binding on member countries and aim to prevent illegal activities and develop national legal systems to combat money laundering, terrorist financing, the proliferation of weapons of mass destruction, and other financial crimes.

(3) In addition to FATF recommendations and national regulations on AML/CFT/CPF, the Bank also considers recommendations, principles, standards, and regulations issued by international regulatory bodies and country authorities (such as the EU, UN, OFAC, HM Treasury, and the Wolfsberg Group), provided they do not contradict national legislation.

3. PURPOSE

(1) The Policy aims to ensure Türk Eximbank's compliance with obligations related to the Prevention of Laundering Proceeds of Crime, Financing of Terrorism, and Financing of the Proliferation of Weapons of Mass Destruction. It seeks to evaluate customers, transactions, and services with a risk-based approach, formulate strategies to reduce risk exposure, determine controls and measures, outline systemic operational steps and responsibilities, and inform the Bank's employees on these issues.

4. DEFINITIONS AND ABBREVIATIONS

(1) The definitions and abbreviations used in this Policy are listed below.

a) **US Department of the Treasury Office of Foreign Assets Control (OFAC):** refers to the organization operating under the US Treasury Department, established to ensure the national security of the US, protect against threats to its foreign policy and economy, and impose economic and trade sanctions in this field.

b) **Laundering:** refers to taking assets arising from a crime out of the country or subjecting them to various transactions to conceal their illegitimate origin and give the impression that they were obtained through legitimate means.

c) **Ministry:** refers to the Ministry of Treasury and Finance of the Republic of Turkey.

ç) **Bank:** refers to Türkiye İhracat Kredi Bankası Anonim Şirketi.

d) **Banking Regulation and Supervision Agency (BRSA):** refers to the public institution with administrative and financial autonomy that regulates and supervises the banking sector.

e) **Unit:** refers to the units of the Head Office, including Liaison Offices, Branches, Regional Directorates, internal systems units, representative offices existing or to be established, and all units in subsidiaries existing or to be established in the future, regardless of the shareholding interest, within the body of Türkiye İhracat Kredi Bankası Anonim Şirketi.

f) **The United Kingdom's Department of Finance and the Economy (HM Treasury):** refers to the department responsible for developing and implementing the UK Government's public finance policy and economic policy and keeping public spending under control.

g) **UNSC:** refers to the United Nations Security Council.

ğ) **Audit Personnel:** refers to Tax Inspectors, Treasury and Finance Experts employed by MASAK, Trade Inspectors, Sworn Bank Auditors, Treasury Controllers, Insurance Supervisors and Actuaries, Experts of the Banking Regulation and Supervision Agency and Capital Markets Board, and Auditors and Experts of the Central Bank of the Republic of Turkey.

h) **Financial Institution:** refers to banks, institutions other than banks authorized to issue debit or credit cards, authorized institutions specified in the foreign exchange legislation, financing and factoring companies, capital market intermediary institutions and portfolio management companies, payment institutions and electronic money institutions, investment trusts, insurance, reinsurance and pension companies and insurance and reinsurance brokers, financial leasing companies, institutions providing clearing, settlement and custody services within the framework of capital markets legislation, precious metals intermediary institutions, and all financial institutions limited to banking activities, including Posta ve Telgraf Teşkilatı Anonim Şirketi.

i) **Fund:** refers to money or any movable or immovable, tangible or intangible, goods, rights, receivables, and all kinds of documents representing them, the value of which can be represented by money.

j) **Beneficial Owner:** refers to the natural persons who perform transactions before the obligor, the natural person or persons who control or have ultimate influence over the natural person, legal entity, or unincorporated entities on whose behalf the transaction is performed.

k) **OECD - Organization for Economic Cooperation and Development:** refers to the international organization established in 1961 to promote global economic cooperation and development, to which Turkey is a party.

l) **Countries/Regions Subject to Comprehensive Sanctions:** refers to countries and/or regions subject to nationwide or regional sanctions imposed by the Republic of Turkey, the United Nations Security Council, the United States of America, the European Union, and the United Kingdom.

m) **CPT:** refers to Countering Proliferation Financing.

n) **Financial Action Task Force (FATF):** refers to the international organization established within the OECD to combat money laundering, financing of terrorism, and proliferation of weapons of mass destruction.

o) **Financial Crimes Investigation Board (MASAK):** refers to the Financial Intelligence Unit (FIU) under the Ministry of Treasury and Finance established to prevent laundering of proceeds of crime, financing of terrorism, and financing of the proliferation of weapons of mass destruction. It conducts research, develops measures, processes the information collected on these crimes, and submits it to the necessary authorities.

p) **Assets:** refer to the funds and income in the ownership or possession or under the direct or indirect control of a natural or legal person, as well as the interest and value derived therefrom or resulting from their conversion. It also includes the funds and income in the ownership or possession of a natural or legal person acting on their behalf or account, and the interest and value derived therefrom or resulting from their conversion.

q) **Freezing of Assets:** refers to the complete removal or restriction of the power of disposition over the assets to prevent their disposal, consumption, conversion, transfer, and assignment.

r) **Regulatory Compliance:** refers to the unit at Turk Eximbank that monitors transactions within the scope of AML/CFT/CPF activities and provides necessary guidance.

s) **Know Your Customer Principle:** refers to all transactions conducted to obtain accurate and sufficient information about customers and Beneficial Owners, to provide and verify the documents specified in the legislation, to monitor transactions, and to ensure that customers' banking activities align with their income, assets, and occupational information.

ş) **Off-Shore Banking**: Off-shore or off-shore banking refers to banking activities conducted through banks established in regions where banking transactions are based on confidentiality, tax advantages, easy transfer opportunities, simple procedures for obtaining a license and establishing a bank, and where financial confidentiality is essential, in addition to offering private banking activities.

t) **Risk:** refers to the likelihood of financial or reputational damage that the Bank or its employees may face due to the use of services for laundering proceeds of crime or financing terrorism, or failure to fully comply with legal obligations, and the risks the Bank may encounter within the scope of compliance activities.

u) **Risky Countries:** refers to countries that do not have adequate regulations on preventing money laundering and terrorist financing, do not cooperate in combating these crimes, or are deemed risky by authorized international organizations, as announced by the Ministry.

ü) AML: refers to the Anti-Money Laundering.

v) **Insured:** refers to the customer benefiting from the Bank's Insurance Programs.

y) **Politically Exposed Persons- PEPs:** refers to individuals holding higher-level public office, such as heads of state or government, senior politicians, government officials, judicial or military personnel, political party representatives in prominent positions, and heads of public institutions.

z) **Relative Close Associate of a Politically Exposed Person:** refers to relatives (spouse, children, siblings, parents), friends, and business associates of politically exposed persons.

aa) **Proceeds of Crime:** refers to the value of assets derived from all kinds of crimes.

bb) **Laundering of Proceeds of Crime:** refers to the transactions aimed at legitimizing earnings obtained through illegal means by introducing them into the financial system, particularly by converting them from cash and changing their identity through a process within the financial system to make them appear as if they were obtained legally.

cc) **Suspicious Transaction:** refers to the presence of any information, suspicion, or reason to suspect that the assets involved in a transaction made or attempted in or through the Bank have been obtained illegally or used for illegal purposes, including for terrorist acts or by terrorist organizations, terrorists, or terrorist financiers, or are related to or connected with them.

dd) **Continuous Business Relation:** refers to the business relationship established between the liable party and the customer due to services such as account opening, credit or credit card issuance, safe deposit box, financing, factoring, financial leasing, life insurance, or personal pension.

ee) **Shell Bank:** Refers to banks that do not have a physical service office in any country, do not employ full-time staff, and are not subject to the supervision and authorization of an official authority in terms of banking transactions and records.

ff) **Financing of Terrorism (FT):** refers to the activity of providing or collecting money or any goods, rights, receivables, income, and benefits that can be represented by money, knowing and willingly that they will be used wholly or partially in the commission of terrorist crimes.

gg) **Compliance Officer:** refers to the officer appointed by the liable parties with the necessary authority to ensure compliance with the obligations imposed by the Law on AML/CFT/CPF and the related legislation, effectively the unit manager responsible for regulatory compliance activities.

hh) **Executives:** refers to executives specified in subparagraph (jj) of the first paragraph of Article 3 of the Regulation on Internal Systems and Internal Capital Adequacy Assessment Process of Banks.

ii) **Senior Management:** Refers to directors specified in subparagraph (kk) of the first paragraph of Article 3 of the Regulation on Internal Systems and Internal Capital Adequacy Assessment Process of Banks.

jj) **Wolfsberg Group:** refers to the organization formed by 13 global banks that aims to develop standards for banks to combat financial crime and sanctions.

kk) **Sanction:** refers to the regulations targeting countries, individuals, and organizations, either individually or comprehensively, to restrict or prevent economic activities to achieve economic and political objectives.

ll) **Prohibited Persons and Entities:** refers to individuals and organizations listed on the UNSC Consolidated Sanctions List, the prohibited/sanctions lists published by OFAC, the EU Consolidated Financial Sanctions List, the UK Consolidated List of Financial Sanctions Targets, the National Lists, and other similar sanctions lists published by international authorities for money laundering and terrorist financing.

mm) **Prohibited Transactions and Activities:** refers to the prohibited transactions and activities included in the UNSC Consolidated Sanctions List, the lists of prohibited persons published by OFAC, the EU Consolidated Financial Sanctions List, the UK Consolidated List of Financial Sanctions Targets, National Lists, and other similar sanctions lists published by international authorities on the grounds of money laundering and terrorist financing, and within the scope of Law on the Prevention of Financing of Weapons of Mass Destruction No. 7262.

nn) **Regulation (Measures Regulation):** refers to the Regulation on Measures for Prevention of Laundering Crime Revenues and Financing of Terrorism.

5. RISK MANAGEMENT

(1) Within the framework of the "Know Your Customer" principle at our bank, it is essential to identify customers and those acting on their behalf and to reveal the Beneficial Owner of transactions. Risk management aims to identify, assess, monitor, evaluate, mitigate, and manage the risks that the Bank may face.

5.1. Customer Acceptance Principles

(1) The Bank's customer acceptance practices for preventing money laundering and terrorist financing are based on the "Know Your Customer" principle. In this context, the Bank is responsible for identifying customers, recognizing the Beneficial Owner, taking the measures specified in the Regulation on Measures Regarding AML/CFT/CPF for risky customers, activities, and transactions that require special attention, recording declared addresses, obtaining additional identifying information and documents specific to the

Bank's internal practices, verifying this information, and storing records in physical and/or electronic form pursuant to the legislation on the prevention of laundering proceeds of crime and financing of terrorism.

(2) In transactions conducted or intermediated by the Bank, it is mandatory to verify the identities of the individuals involved and those on whose behalf or accounts the transactions are made before the transaction is executed. In case of non-compliance, MASAK will impose sanctions on the Banks as specified in the relevant articles of Law on Prevention of Laundering Proceeds of Crime No. 5549.

(3) Before establishing a business relationship or conducting a transaction at the Bank, personnel directly dealing with the customer must verify the customer's identity as specified in the Regulation on Measures. The following considerations are taken into account:

a) In identification and confirmation procedures, necessary checks are carried out as follows:

- Regardless of the amount when establishing a permanent business relationship,
- When the transaction amount or the total amount of multiple interconnected transactions meets or exceeds the threshold specified in subparagraph (b) of the first paragraph of Article 5 of the Regulation on Preventive Measures for Laundering Proceeds of Crime and Financing of Terrorism,
- In wire transfers, when the transaction amount or the total amount of multiple interconnected transactions meets or exceeds the threshold specified in subparagraph (c) of the first paragraph of Article 5 of the Regulation on Preventive Measures for Laundering Proceeds of Crime and Financing of Terrorism,
- Regardless of the amount in cases requiring suspicious transaction reporting,
- Regardless of the amount when there is doubt about the adequacy and accuracy of previously obtained customer identification information.

b) Within the scope of the "Know Your Customer" principle, necessary checks are carried out before initiating a permanent business relationship on the following matters:

- Identification and address detection,
- Customer's business/professional information,
- Customer's core business,
- Information and documents related to the insured or the insured asset,

- Internal consistency of documents and information,
- Customer’s transaction profile and capacity,
- Its buyers and sellers,
- Identification of the Beneficial Owner,
- Workplace or place of activity,
- Sufficient information about the purpose and nature of the requested transaction.

c) In the identification and registration of the declared address, the following points are observed:

- Identity and address are determined and confirmed according to the documents and obligations specified in the Measures Regulation. The accuracy of the information is cross-checked using the MERNIS system, the information on Tax Identification Numbers from the Republic of Turkey Ministry of Treasury and Finance (electronically obtained from the Revenue Administration), and the identity sharing system database of the General Directorate of Civil Registration and Citizenship Affairs, by applying to the relevant trade registry office records, or by querying the database of the Union of Chambers and Commodity Exchanges of Turkey.
- Identifying the insured is essential at the policy issuance stage. At the indemnity payment stage, the identities of the insured, the buyer, and, to the extent possible, other parties related to the transaction are also verified.
- The identity and authorization of those declaring they act on behalf of the customer are determined. Powers of attorney must be notarized, and non-original instructions and documents must be notarized to the extent possible.
- Attention is paid to the consistency of documents and information.
- Records and documents related to customer information are stored electronically and kept accessible to authorized persons.
- A readable photocopy or electronic image is taken after the submission of the original or notarized copies of the documents that are the basis for confirmation, or identity information is recorded to be presented when requested by authorized persons.

It is not sufficient to obtain the relevant documents once from customers with whom a continuous business relationship is established; information must be kept up to date.

Necessary measures are taken to determine whether the customer is acting on behalf of someone else and the Beneficial Owner of the transaction. If it is suspected that the person is acting on behalf of someone else despite declaring otherwise, a reasonable investigation is conducted to reveal the Beneficial Owner.

ç) For legal entities, the following three main points are considered to identify the Beneficial Owner:

- Ownership (shareholding) relationship,

- Final control, and

- High-level representation authority.

d) The steps to identify the Beneficial Owner are as follows, respectively:

- When establishing a permanent business relationship with legal entities registered in the trade registry, the identity of the natural person partners with shares exceeding twenty-five percent of the entity must be identified and confirmed to determine the Beneficial Owner.

- If it is suspected that the natural person partner with shares exceeding twenty-five percent is not the Beneficial Owner, or if there is no natural person partner with such shares, the natural person(s) who ultimately control the entity should be identified and their identities confirmed.

- If the Beneficial Owner cannot be identified as described above, the natural person(s) with the highest executive authority registered in the trade registry will be considered the Beneficial Owner. The identification and confirmation of these persons must be conducted.

- When establishing a permanent business relationship with legal entities registered in the trade registry, the identification and confirmation of legal entity partners with shares exceeding twenty-five percent must also be conducted. Confirmation of identity information for legal entity partners residing abroad can be made through open sources from equivalent organizations to the Union of Chambers and Commodity Exchanges of Turkey in the relevant country or other official organizations.

- Representatives of legal entity shareholders with shares exceeding twenty-five percent do not need to be identified, and their signature samples do not need to be obtained.

5.2. Screening Customers and Payments in Sanctions Lists:

(1) All new customers, as well as their authorized representatives and owners of companies and other related persons, are screened against various sanctions lists, including European Union Financial Sanctions, OFAC, United Nations Security Council, United Kingdom (HM Treasury), local sanctions lists (published/shared by MASAK, Ministry of Interior Terrorism Wanted List, etc.), the Bank's internal list, and lists provided by internationally reputable trade organizations that monitor these lists daily.

(2) Economic sanctions are measures taken by international organizations or countries to prohibit the export or import of a good/product or service. Financial sanctions, on the other hand, include measures to limit or completely prohibit financial transactions of the target country, person, or institution. The Bank follows the regulations of international authorities such as the United Nations (UN), the European Union (EU), the United Kingdom (HMT), the United States (OFAC), and local sanctions where it operates and takes necessary measures to comply with these regulations.

(3) These screenings are performed through the software integrated by the Bank into its main banking/insurance systems.

(4) For existing customers, the aforementioned checks are carried out daily based on list updates and at periodic intervals determined by risk factors during the relevant period.

(5) In the surveillance of sanction risks:

- Customers, shareholders, those acting on behalf of the customer, and ultimate beneficiaries are screened against the lists.

- It is examined whether the customer's transactions with or through the Bank involve countries/regions subject to comprehensive sanctions or a sanctioned person or entity.

- No customer acceptance or transaction is made until authorized persons complete the evaluations on the screening results.

- Existing customers are regularly scanned to check if they are included in such lists.

(6) A continuous business relationship shall not be established, and transactions shall not be intermediated with persons and entities included in the lists published by the authorized institutions within the scope of the regulations on Laundering Proceeds of Crime, Financing of Terrorism, and Prevention of Financing the Proliferation of Weapons of Mass Destruction. If it is determined that persons or organizations with whom a continuous business relationship has been established are connected to those on the list, necessary reports are submitted to the relevant authorities. Risks related to the continuous business relationship are also evaluated by Regulatory Compliance.

5.3. Simplified Measures for Customer Identification

(1) The Bank may apply simplified measures in the following transactions within the scope of the Measures Regulation, in accordance with the principles set forth in the Financial Crimes Investigation Board General Communiqué No: 5.

(2) Simplified measures apply to:

- Transactions where the customer is a financial institution (including interbank transactions),

- Transactions where the customer is a public administration or a professional organization in the nature of a public institution within the scope of general government according to the Public Financial Management and Control Law No. 5018,

- Transactions where the customer is a publicly traded company with its shares listed on the stock exchange.

(3) However, simplified measures cannot be applied to transactions that are considered risky in terms of money laundering and terrorist financing. It is ensured that these transactions are forwarded to Regulatory Compliance for report to MASAK.

5.4. Measures for Higher-Risk Customers, Activities, and Transactions Requiring Special Attention

a) **Customer Risk:** This includes the risk that the customer's line of business allows for the intensive use of cash, the purchase and sale of high-value goods, or the easy realization of international fund transfers. It also includes the risk of abuse of obligors due to the fact that the customer or those acting on behalf of the customer may be involved in laundering proceeds of crime or financing terrorism.

b) **Product/Service Risk:** Transactions that are not conducted face-to-face, correspondent banking, products and services offered using developing technology, and products and services that are considered risky due to their nature are categorized as high risk.

c) **Country/Region Risk:** Customers and transactions that are connected to countries/regions where necessary regulations and measures to prevent money laundering or terrorist financing are not taken, where there is inadequate cooperation in combating these crimes, or which are considered risky by international authorities (FATF, UN, OFAC, EU, HM Treasury). This includes countries/regions located on drug production-distribution routes (gray areas), where crimes such as smuggling, terrorism, corruption, and bribery are widespread, and those referred to as tax havens/off-shore centers. This risk is assessed based on nationality, country of birth, country of residence, place of establishment, partnership structure, authorities, and transaction parties.

The Bank is obliged to pay special attention to business relations and transactions with natural and legal persons, unincorporated entities, and citizens of risky countries. The Bank must collect and record as much information as possible about the purpose and nature of transactions that do not have a reasonable legal and economic purpose.

The Bank takes measures determined by the Ministry, including those adopted by international organizations of which Turkey is a member, regarding risky countries.

ç) **Relations with Risky Countries:** Financial institutions must pay special attention to business relations and transactions with natural and legal persons residing in risky countries, entities without legal personality, and citizens of these countries. They must collect and record information to the extent possible about the purpose and nature of transactions that do not have a reasonable legal and economic purpose on the surface.

The Ministry is authorized to determine the measures to be taken regarding risky countries, including those accepted by international organizations of which Turkey is a member.

To rate and mitigate customer risk, Customer Due Diligence (CDD)and customer risk profiles are established within the framework of the Customer Due Diligence (CDD). Persons or organizations that should not be engaged in continuous business relations and require additional measures are determined and all customers are reviewed periodically.

d) **Sensitive Sectors and Business Lines in Laundering Proceeds of Crime:** Special attention is given to providing banking services, particularly in sectors and occupational groups with high cash transaction volumes and easily convertible activities. Customer identity and sector information are meticulously recorded. Under the risk-based approach, additional measures are applied for accepting such customers, monitoring their transactions, and ensuring necessary controls in the product lists created by international authorities (e.g., European Union, United Kingdom, USA).

Our Bank considers companies involved in producing/trading dual-use and sensitive materials and technologies that could potentially be used in the development of weapons of mass destruction as risky. These companies are subjected to detailed examination and monitoring, regardless of their inclusion in lists like the Wassenaar Arrangement Dual-Use Material and Technology list or the Australian Group Chemical Precursors List.

e) **Transactions Requiring Special Attention:** Special attention is given to complex and unusually large transactions and those without a reasonable legal and economic purpose. Necessary measures are taken to obtain sufficient information about the purpose of the requested transaction.

f) **Taking Measures Against Technological Risks:** The Bank pays special attention to the risk of using new and developing technologies for laundering and terrorist financing and takes appropriate measures to prevent this. The Bank closely monitors non-face-to-face transactions, ensures transactions align with the customer's activities and implements effective measures, including setting limits on transaction amounts and frequency.

g) **Politically Exposed Persons (PEP) and their Relatives (RCAs):** It is determined whether there are politically exposed persons in the customer's management and/or persons with close relatives or business connections with any politically exposed person. Reasonable research is conducted to learn the source of funds and assets, necessary measures are taken if a match is found, and establishing a business relationship is decided with the approval of the relevant unit's manager.

ğ) **Correspondent Relationship:** Correspondent banking transactions are high-risk.

Before establishing a correspondent relationship:

- Reliable information should be obtained from publicly available sources to determine if the counterparty financial institution is under investigation for money laundering or terrorist financing, whether it has been fined or warned, the nature and subject matter of its business, its reputation, and the adequacy of its supervision.

- The correspondent financial institution's AML/CFT system should be evaluated to ensure it is appropriate and effective.

- It should be ensured that the relevant correspondent does not work with so-called "shell banks" and does not allow its accounts to be used by these banks.

- The approval of the senior manager of the relevant unit should be obtained before establishing new correspondent relationships.

- Sufficient and satisfactory information and documents regarding policy implementation and controls on the prevention of laundering proceeds of crime and financing of terrorism

should be obtained from counter financial institutions with which a correspondent banking relationship will be established.

For this purpose, the relevant departments should request the financial institutions seeking to open correspondent accounts to fill out a questionnaire prepared by the Wolfsberg Group, which is not older than one year. This questionnaire should include information such as the subject of business, title, measures taken to prevent money laundering, and the name of the compliance officer.

h) **Reliance on Third Parties:** Financial institutions may establish a business relationship or conduct a transaction by relying on another financial institution's measures to identify the customer, the person acting on behalf of the customer, and the beneficial owner and to obtain information about the business relationship or transaction's purpose. However, the ultimate responsibility for AML/CFT/CPF compliance remains with the financial institution, which relies on the third party.

Provided the third party has taken identification, record keeping, and other measures to ensure the requirements of the Customer Due Diligence (CDD) , and if it is resident abroad, that it is also subject to international standards, regulations, and audits related to AML/CFT, and that certified copies of identification documents will be provided immediately upon request.

A financial institution establishing a business relationship or conducting a transaction by relying on a third party shall immediately obtain the customer's identification information from the third party.

Transactions between financial institutions on behalf of their customers and their relations with agents and similar units of financial institutions and persons to whom they outsource services that are extensions or complements of their main service units are not covered by the principle of trust in third parties.

The principle of trust in third parties does not apply if the third party is a resident in a country defined as risky by this policy.

Information requests from Account Correspondents or other financial institutions with which the Bank has business relations regarding the regulations on the Bank's practices on AML/CFT/CPF are fulfilled by Compliance.

In order to prevent any disruption in communication and any deficiencies in the records, such applications are made with the knowledge and through the relevant departments managing correspondent relations.

5.5. Enhanced Measures for Highly Risky Groups

In our Bank, the following additional measures may also be applied to higher-risk customers and higher-risk situations identified under a risk-based approach:

- Obtaining additional information about the customer and updating their identity information and that of the Beneficial Owner more frequently.

- Obtaining additional information about the nature of the business relationship.

- Obtaining as much information as possible about the source of the assets subject to the transaction and the customer's funds.

- Obtaining information about the transaction's purpose.

- Requiring higher-level official approval for entering into a business relationship, maintaining an existing relationship, or executing a transaction.

- Keeping the business relationship under close supervision by increasing the number and frequency of controls applied and identifying transaction types requiring additional controls.

- Requiring the first financial transaction in establishing a continuous business relationship to be made from another financial institution that applies Customer Due Diligence (CDD).

5.6. Individuals and Organizations Not Accepted as Customers

(1) Our Bank shall not engage in any transactions aimed at circumventing sanctions with individuals and organizations included in the sanctions lists (OFAC List, UN Consolidated List, United Kingdom, European Union, etc.) published by authorized institutions, in addition to national legislation within the scope of the prevention of Laundering Proceeds of Crime, Prevention of Financing of Terrorism, and Prevention of Financing of Proliferation of Weapons of Mass Destruction.

(2) If it is determined that the individuals or organizations with whom a continuous business relationship has been established have a connection with the individuals or organizations whose names are included in the sanctions lists, necessary reports shall be submitted to the relevant units. The termination of the continuous business relationship will be evaluated by the relevant department.

(3) Transactions of shell banks and shell companies that do not physically exist, are not subject to the supervision and permission of any official authority and do not have adequate regulations on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism shall not be intermediated directly or indirectly.

(4) Transactions of individuals and organizations that refrain from submitting the information and documents requested during the establishment of a permanent business relationship, refrain from filling in the information forms and provide misleading and unverifiable information shall not be intermediated.

(5) Individuals and organizations that have a bad reputation for laundering proceeds of crime and financing terrorism at the international level, and banks located in countries that are generally accepted to have poor reputations and weak controls and examinations, will not have their high-value policies, checks, or letters of guarantee issued on or by these banks processed.

It is important for the national and international reputation of the Bank not to enter into such business relations.

(6) Necessary measures are taken and meticulously implemented to avoid entering into business relations with prohibited persons and organizations included in the lists published by the United Nations Security Council for the prevention of financing of terrorism and the proliferation of weapons of mass destruction, which are binding for our country with the Presidential Decree published in the Official Gazette, as well as other international lists such as these, which should be taken into consideration by the banks of our country as well as the international financial system, and within the scope of prohibited transactions and activities within this scope.

(7) Individuals and organizations that directly or indirectly control the individuals and organizations included in the aforementioned lists, as well as those acting on their behalf or account or collecting or providing any kind of funds for their benefit, are also considered within the same scope.

(8) Individuals whose ownership structure is so complex that the reason cannot be understood and whose Beneficial Owner cannot be identified are not considered as customers.

5.7. Circumstances Requiring Rejection of Transaction and Termination of the Business Relationship

(1) In cases where the identification of customers cannot be made and/or sufficient information cannot be obtained about the purpose of the business relationship, the business relationship shall not be established.

(2) In cases where the required identification and confirmation cannot be made due to doubts about the adequacy and accuracy of the previously obtained customer identification information, no new products and services are offered to the relevant customer by the Bank. Whether the said situation is a suspicious transaction or not is also evaluated separately.

6. MONITORING AND CONTROL OBLIGATION

(1) The Bank carries out monitoring and control activities with a risk-based approach by taking into account the nature of customers' transactions. The purpose of monitoring and control activities is to protect the Bank from risks and to continuously monitor and control whether the Bank's activities are carried out in accordance with the Law on AML/CFT/CPF and the regulations and communiqués issued pursuant to the Law and the policies and procedures of the institution.

(2) In this context, the monitoring and control activities to be carried out at the Bank within the framework of the relevant legislation cover the following issues:

- Monitoring and control of customers and transactions in the higher-risk group,
- Monitoring and control of transactions with higher-risk countries,
- Monitoring and control of complex and unusual transactions,
- Checking the information and documents that must be kept electronically or in writing about customers and the information required to be included in wire transfer messages through sampling and having the deficiencies completed and updated,
- Continuously monitoring whether the transactions carried out by its customers are in line with the information on its customers' profession, commercial activities, business history, financial status, risk profile, and fund sources throughout the business relationship and keeping the information, documents, and records about its customers up to date,
- Controlling transactions carried out using methods or systems that enable non-face-to-face transactions,
- Risk-oriented control of services that may become vulnerable to abuse due to new products and technological developments,
- Monitoring the news reflected in the media regarding the laundering of proceeds of crime or financing terrorism and examining whether the persons mentioned in the relevant news are customers of the Bank.

(3) Monitoring customer status and transactions, continuously monitoring whether the transactions carried out by customers within the scope of a continuous business relationship are compatible with the information on the customers' commercial activities, business history, financial status, risk, and fund sources, and keeping the information, documents, and records on the customer up-to-date.

(4) In the event that individuals and organizations included in the international prohibited lists

are included in the said lists among new customers/existing customers during the controls performed during customer acceptance/at the time of transaction, or in case of a request for transactions that are not in line with the purpose of establishing the declared business relationship and customer profile, the status of the customer, the nature of the transactions, and the content of the business relationship are examined by Regulatory Compliance.

7. SUSPICIOUS TRANSACTIONS

(1) If there is any information, suspicion, or reason to suspect that the money or values represented by the money involved in transactions conducted or attempted through our Bank have been obtained illegally, used for illegal purposes, used by terrorist organizations and financiers, used for terrorist acts, or linked to terrorism in any way, a Suspicious Transaction Report shall be submitted to MASAK about the individuals involved in the transaction, regardless of any monetary limit.

7.1. Detection and Reporting of Suspicious Transactions

(1) Suspicious Transaction Reports are confidential; therefore, no one, including the parties to the transaction, shall be informed that a Suspicious Transaction Report has been or will be made to MASAK, except for information provided to the audit staff assigned with liability audit and to the courts during proceedings.

(2) Pursuant to Article 10 of the Law on AML, the Bank's legal entity and personnel who fulfill the obligation to report suspicious transactions shall not be held legally or criminally liable for having reported suspicious transactions.

(3) The Compliance Officer shall conduct the necessary investigation regarding the Suspicious Transaction Reporting and submit a report in accordance with the legislation within ten business days at the latest from the date of suspicion regarding the transaction.

(4) If new information and findings are obtained later regarding the notified transaction, the Suspicious Transaction Report Form shall be filled out again and reported to MASAK without delay, stating that it is in addition to the previous report. Therefore, it is important to pay special attention to and conduct enhanced ongoing monitoring the reported customers.

(5) The types of suspicious transactions listed in the Suspicious Transaction Reporting Guide published by MASAK should not be considered the only criteria. A suspicious transaction may be reported even if it does not comply with any of the types specified in the Suspicious Transaction Reporting Guide.

(6) In the transactions conducted, the following issues can be listed as the main factors that constitute a reason for reporting suspicious transactions:

- The willingness of the customer to provide personal information,

- No apparent legal or economic purpose,

- Providing misleading information, documents, and contact information,
- Requesting loans against cash that have no intended use and where the intended use is not specified,

- Providing misleading, insufficiently explained, and unverifiable information,

- Requesting credit/insurance with documents such as contracts that are not relevant and proportionate to the customer's income and job,

- Making an insurance claim with forged documents,

- Export documents are deemed to be forged,

- Complex and unusually large transactions and transactions that do not have any apparent reasonable legal and economic purpose.

(7) In such cases, a Suspicious Transaction Reporting Form must be prepared and submitted directly to the Regulatory Compliance (Compliance Officer) without delay. Reports should be submitted via e-mail or internal correspondence (EBYS).

(8) While investigating the suspicious transaction before the report, attitudes, and behaviors that may cause the customer to suspect that a report will be submitted about him/her should be avoided.

(9) Additionally, suspicious transactions detected during the controls/audits conducted by the Internal Control Department and the Board of Internal Auditors are reported to the Regulatory Compliance (Compliance Officer) to be subject to report regardless of the amount.

(10) It is the fundamental responsibility of all units to submit the information and documents requested from the Units by the Compliance Officer in a timely, complete, and suspicion-free manner.

(11) The Compliance Officer is authorized and responsible for deciding whether or not to send a Suspicious Transaction Report to Regulatory Compliance. In cases where the notifications received from the units are not required to be notified to MASAK by the Compliance Officer, the Compliance Officer shall make and keep a written decision justifying his/her opinion.

(12) The Suspicious Transaction Reporting Form, which is decided to be notified, shall be transmitted to MASAK by an appropriate and provable method.

(13) In the event that a Suspicious Transaction Reporting is not made about a transaction that should be suspected pursuant to the Law on Prevention of Laundering Proceeds of Crime, an administrative fine shall be imposed on both the Bank's legal entity and the personnel who execute, approve, and fail to notify the transaction in the amounts specified in the relevant regulations per transaction.

(14) The Bank's legal entity and personnel who fulfill the suspicious transaction reporting obligation shall not be held legally and criminally liable in any way due to the fact that they have reported suspicious transactions.

(15) In the event that any information regarding suspicious transaction reporting is disclosed to third parties, those who provide such information shall be subject to imprisonment and judicial fines as specified in the Law on AML.

7.2. Postponement of Transaction Based on Suspicious Transaction Reporting

(1) If there are documents or serious indications supporting the suspicion that the assets subject to the transaction attempted or currently ongoing at or through the Bank are related to the crime of laundering or financing of terrorism, the suspicious transaction reporting must be sent to MASAK with a request to postpone the transaction together with the reasons.

(2) If suspicious transaction reports are sent to MASAK with a request to postpone the transaction, the realization of the transaction shall be refrained from until the decision to be made about the transaction is notified to the Bank by MASAK. The postponement of the transaction is seven business days from the date of the Suspicious Transaction Report.

8. OTHER LIABILITIES

(1) The Bank adopts a risk-based approach to prevent both terrorism financing and money laundering, aiming to avoid abuse and minimize risks related to terrorism financing.

(2) The Bank does not collect or provide funds nor engage in business partnerships or other business relations within Turkey with or for the benefit of persons or entities specified in the UNSC resolutions and annexes referred to in Law on the Prevention of Financing of Terrorism No. 6415 and Law on the Prevention of Financing the Proliferation of Weapons of Mass Destruction No. 7262. This also applies to those directly or indirectly controlled by them or acting on their behalf or account.

(3) The Bank shall not establish business partnerships with financial institutions of the persons, entities, or organizations specified in these resolutions, nor with those controlled by them or acting on their behalf. Additionally, the Bank shall not provide any financial services,

establish a correspondent relationship, or continue an existing one if applicable.

(4) Pursuant to the Law on the Prevention of Weapons of Mass Destruction and the Law on the Prevention of Financing of Terrorism, asset freezing and removal decisions made by the President shall be published in the Official Gazette. These decisions are considered notified to the relevant persons, institutions, or organizations on the date of publication.
Decisions published in the Official Gazette are communicated within the Bank via e-mail by Compliance. The Bank must notify MASAK without delay, or within seven days at the latest, confirming whether it holds any assets in its custody and providing other relevant information.

(5) Failure to comply with asset freezing decisions as stipulated in Law on the Prevention of Financing of Terrorism No. 6415, or any negligence or delay in fulfilling these decisions, shall result in an administrative fine on the Bank's legal entity, as specified in the Law, with an annual increase based on the revaluation coefficient.

(6) Except for cases authorized by MASAK, those whose assets are frozen cannot carry out transactions that eliminate, consume, transform, transfer, assign, or otherwise dispose of these assets. Such transactions cannot be facilitated or enabled.

9. BANK'S APPROACH UNDER AML/CFT/CPF

(1) Although the Bank is not among the obliged institutions in the implementation of the AML law per Article 4 of the Regulation on Measures for Prevention of Laundering Crime Revenues and Financing of Terrorism, it complies with national legislation, legal regulations, and international standards in the fight against AML/CFT/CPF. The Bank takes the following measures within its awareness to ensure effective controls in this context:

- Establishing policies and procedures
- Conducting risk management, monitoring, and control activities
- Appointing a compliance officer and establishing a compliance unit
- Implementing training activities
- Executing internal audit activities.

(2) The duties, authorities, and responsibilities of the Compliance Officer include:

- Ensuring compliance with the Law and related regulations regarding AML/CFT/CPF at the Bank and maintaining communication and coordination with MASAK,
- Establishing policies and procedures under relevant legislation and submitting them for

approval to the Board of Directors through the Audit Committee or directly,

- Evaluating information and findings on transactions that may be suspicious, as communicated or learned *ex-officio*, conducting necessary investigations within the scope of authority and capability, and notifying MASAK of suspicious transactions,

- Taking measures to ensure the confidentiality of reports and related matters,

- Ensuring communication and coordination with MASAK and providing requested information and documents,

- Responding to letters from MASAK regarding asset freezing and lifting decisions under Presidential Decrees,

- Collaborating with Human Resources on training within the scope of AML/CFT/CPF and supporting the effective implementation of the training program,

- Conducting risk management, monitoring, and control activities considering the risks identified within national/product risk assessments and ensuring necessary communication and coordination with MASAK.

(3) The Compliance Officer, reporting to the Board of Directors through the Audit Committee, carries out these activities.

10. OBLIGATION TO PROVIDE INFORMATION AND DOCUMENTS

(1) Every effort must be made to promptly provide all types of information, documents, and their records in all forms of media requested by MASAK and its auditors, including necessary information and passwords to access or render these records readable, ensuring completeness and accuracy, in the manner, format, and within the timelines specified.

(2) Information may be requested verbally or in writing. In order to prevent communication failures and record deficiencies, such requests must involve the department relevant to the request, with follow-up conducted by the respective department.

(3) It is mandatory, under applicable laws, to furnish all requested information and documents to MASAK and auditors. Violations of the continuous information provision obligation or the obligation to provide information/documents may result in fines and/or imprisonment penalties as stipulated in the relevant laws.

11. RECORD KEEPING

(1) Pursuant to the law, the Bank shall retain all information and documents acquired during the periods specified under relevant legislation for submission when required. This obligation includes the preservation and submission of suspicious transaction reporting.

(2) In all media types concerning obligations and transactions imposed on the Bank by the law:

- Documents from the date of issuance,
- Books and records from the date of last entry,
- Documents related to identification from the date of the last transaction,

must be preserved for eight years and submitted to authorities upon request.

(3) Penalties specified in relevant laws apply to violations of the aforementioned record retention provisions.

12. TRAINING

(1) The training policy aims to ensure compliance with legal obligations, regulations, and directives issued under the law, cultivate a corporate culture by enhancing personnel awareness of responsibility towards corporate policies, procedures, and a risk-based approach, and update personnel knowledge.

(2) AML/CFT/CPF training activities are coordinated and supported by the Compliance Officer. Training subjects, employees, and trainers are to be trained, and the annual training program is determined by the Compliance Officer and Human Resources and conducted using appropriate methods (online/classroom/informational, etc.) within the annual training program.

13. INTERNAL AUDIT

(1) The purpose of internal audit under this Policy is to provide independent/objective assurance to the Board of Directors regarding the effectiveness, adequacy, and compliance of all compliance activities. Internal audit activities aim to audit the effectiveness, adequacy, and efficiency of corporate policies and procedures, risk management, monitoring and control activities, training activities, risk policy, compliance of Bank transactions with AML Law and regulations, directives, and corporate policies and procedures issued under the law, and the proper execution of compliance activities with a periodic and risk-based approach.

(2) Deficiencies, errors, and misconduct identified through internal audit, along with opinions and suggestions for preventing their recurrence reported by the Internal Audit Board, are addressed through monitoring activities conducted by the Internal Audit Board and reported directly to the Board of Directors or through the Audit Committee.

(3) Actions taken in response to opinions and suggestions reported by the Internal Audit Board and the results of related activities are reported to the Board of Directors through the Audit Committee or directly by the Compliance Officer.

(4) Compliance with this Policy is ensured through controls implemented in audits conducted by the Internal Audit Board at units performing relevant activities and/or audits specified in the risk-based annual audit plan. When determining the scope of audits related to Policy compliance, audits may include failures in monitoring and control activities, customers, services, and transactions posing a risk, reported to or identified by relevant stakeholders within the framework of the Internal Audit Regulations and relevant regulations.

(5) The size and transaction volume of the Bank are considered when determining areas to be audited by the Internal Audit Board. Thus, audits are aimed at covering units and transactions of the Bank in terms of quantity and quality to address areas of highest risk from a risk-oriented perspective.

14. ENFORCEMENT and EXECUTION

(1) The Policy on Prevention of Laundering Proceeds of Crime, Financing of Terrorism and Proliferation of Weapons of Mass Destruction shall take effect upon approval by the Bank's Board of Directors.

(2) The Policy is reviewed annually to maintain compliance with legislation and international standards, and updates are made as necessary and submitted to the Board of Directors for approval.

(3) All parties are responsible for implementing the provisions of this document within the scope of their duties.

(4) Compliance with the provisions of this Policy is overseen by Regulatory Compliance.