TÜRKİYE SINAİ KALKINMA BANKASI A.Ş.
POLICY ON THE PREVENTION OF LAUNDERING PROCEEDS OF CRIME, FINANCING OF TERRORISM AND PROLIFERATION FINANCE

FIRST PART
Purposes, Legal Grounds and Definitions

Purpose and Scope

Article 1 - Türkiye Sınai Kalkınma Bankası A.Ş. ("the Bank") attaches critical importance to preventing the laundering of proceeds of crime and the financing of terrorism and proliferation finance and aims to fully comply with national and international legislation and standards on sanctions programs. The Bank also sees this effort as a key element of harmonization with the international system within the framework of the cooperation it has developed with supranational and international financial institutions and development finance institutions.

The main purposes of the Policy on the Prevention of Laundering Proceeds of Crime, Financing of Terrorism and Proliferation Finance ("Policy") are to implement the Compliance Program, which is established with a risk-based approach to ensure the Bank's compliance with the obligations set by national legislation on the prevention of laundering proceeds of crime, financing of terrorism and proliferation finance, taking into account international recommendations, standards and best practices, to evaluate customers, transactions and services in accordance with the principle of risk-based approach to identify strategies, controls and measures, operating rules and responsibilities to mitigate and control risks, including reputational risk, to which the Bank may be exposed, and to raise and improve the awareness of the Bank's employees on combating financial crimes and on sanctions, thus reinforcing the corporate culture.

This Policy covers all departments, branches and employees of the Bank.

Legal Grounds

Article 2 - This Policy has been prepared under the supervision and coordination of the Compliance Officer, with the participation of all relevant Bank departments and in line with the Law No. 5549 on the Prevention of Laundering Proceeds of Crime promulgated in the Official Gazette No. 26323 dated October 18, 2006 and the regulations related thereto, the Law No. 6415 on the Prevention of Financing of Terrorism promulgated in the Official Gazette No. 28561 dated February 16, 2013 and the regulations related thereto, the Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction promulgated in the Official Gazette No. 31351 dated December 31, 2020 and the regulations related thereto, the National Risk Assessment, the FATF Recommendations setting the International Standards, and the Wolfsberg Principles.

Abbreviations and Definitions

Article 3 - For the purposes of this Policy,

"Assistant Compliance Officer" refers to the Bank employee who reports to the Compliance Officer to execute the Compliance Program and meets the conditions and qualifications required for the Compliance Officer to fulfil the duties specified in the relevant legislation,

"Assets" refer to money, any kind of movable or immovable, tangible or intangible goods or rights which have monetary value, and any kind of legal documents or instruments certifying rights on them, and/or funds and proceeds partially or completely owned or possessed or directly or indirectly controlled by a natural person or legal entity, and any benefit and value obtained from them or derived from the interconversion of them, and/or funds and proceeds partially or completely owned or possessed by a natural person or legal entity acting on their behalf or in their name, and any benefit and value obtained from them or derived from the interconversion of them,

"Bank" refers to Türkiye Sınai Kalkınma Bankası A.Ş.,

"Beneficial Owner" refers to natural person(s) who ultimately control(s) or own(s) natural persons who carry out a transaction within the Bank, or the natural persons, legal persons or unincorporated organizations on whose behalf a transaction is being conducted,

"Board of Directors" refers to the Board of Directors of Türkiye Sınai Kalkınma Bankası A.Ş.,

"Compliance Officer" refers to the Bank employee who is employed to report to the Board of Directors for the purpose of ensuring the compliance with obligations established through the Law on the Prevention of Laundering Proceeds of Crime or the legislation issued on the basis of this Law and who is entrusted with the required authority,

"Compliance Program" refers to the whole set of measures established within the Bank in line with the relevant legislation and the Bank Policy for the prevention of laundering of proceeds of crime and the financing of terrorism,

"Compliance Unit" refers to the unit comprised of employees reporting to the compliance officer and responsible for the execution of the compliance program,

"Country Risk" refers to the risk which is possible to be exposed by obliged parties due to business relationships and transactions with citizens, companies and financial institutions of the countries that lack appropriate money laundering and financing of terrorism laws and regulations, being non-cooperative in the fight against these offences or being identified by competent international organizations as risky,

"Customer Risk" refers to the risk for the Bank to be abused due to the business field of the customer allowing intensive cash flow, purchasing of valuable goods or international fund transfers to be carried

out easily, and due to the acts of customer or those acting on behalf or for the benefit of the customer for money laundering or terrorist financing purposes,

“Examiner” refers to examiners set forth in the Law No. 5549 on the Prevention of Laundering Proceeds of Crime and the regulations related thereto, including Tax Inspectors, Treasury and Finance Experts who are employed at the Presidency, Customs and Trade Inspectors, Sworn-in Bank Auditors, Treasury Comptrollers, Insurance Supervisory Experts and Actuaries, Banking Regulation and Supervision Agency Experts and Capital Markets Board Experts, Auditors and Experts of the Central Bank of the Republic of Türkiye,

"FATF" refers to and stands for the Financial Action Task Force,

"Financial Group Policy" refers to the Türkiye İş Bankası A.Ş. Financial Group Policy for Combating Financial Crimes,

“Financial Group” refers to the group consisting of financial institutions resident in Türkiye, affiliated with or under the control of a parent institution headquartered in Türkiye or abroad, and their branches, agencies, representatives, commercial proxies and similar affiliates,

"Freezing of Assets" refers to the removal or restriction of the power of disposition over the asset for the purpose of preventing obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset or restriction within the framework of transactions permitted by MASAK,

"Fund" refers to money or any instruments such as bank credits, bank or traveler’s cheques, money orders, securities, shares, guarantees, bill of exchange, bonds, policies, letter of credits and property, right, claims of every kind whether movable or immovable, tangible or intangible, however acquired, which could be represented by money and all kinds of documents in any form, including electronic or digital, evidencing title to or interest in such assets,

"Laundering of Proceeds of Crime (Money Laundering)" refers to actions and initiatives taken with the intention of incorporating the revenues and proceeds of illegal acts into the financial system for the sake of creating an impression that they have been obtained legally, thereby especially releasing them from cash form, and of making such revenues and proceeds legitimate by changing their identity through a process contained in the financial system itself,

"Legislation" refers to the laws, regulations and communiqués in force regarding the prevention of Laundering Proceeds of Crime, Financing of Terrorism and Proliferation Finance, as well as MASAK resolutions and instructions,

"MASAK" refers to and stands for the Financial Crimes Investigation Board,

"Ministry" refers to the Ministry of Treasury and Finance of the Republic of Türkiye,

"NCCT" refers to and stands for Non-Cooperative Countries and Territories,

"OFAC" refers to and stands for the Office of Foreign Assets Control,

"Parent Financial Institution" refers to Türkiye İş Bankası A.Ş.,

"Permanent Business Relationship" refers to a business relationship that is established between the Bank and its customers through services such as opening an account, lending loan, financing, factoring or financial leasing, and that is permanent due to its characteristics,

"Policy" refers to the Bank's Policy on the Prevention of the Laundering of Proceeds of Crime, Financing of Terrorism and Proliferation Finance,

"Politically Exposed Persons (PEPs)" refer to high-level real persons who are entrusted with a prominent public function by election or appointment domestically or in a foreign country and members of the board of directors, senior executives and other persons who have an equivalent duty of international organizations,

"Prevention of the Financing of the Proliferation of Weapons of Mass Destruction" refers to sanction resolutions of the United Nations Security Council (UNSC) on the prevention of financing the proliferation of weapons of mass destruction,

"Proceeds of Crime" refer to the proceeds derived from crime,

"Sanctions" refer to measures targeting countries, individuals and organizations to restrict or prevent economic activities, either individually or comprehensively, in order to attain economic and political objectives,

"Senior Management" refers to the Bank's Chief Executive Officer and Executive Vice Presidents as well as the managers of departments under Internal Systems,

"Service Risk" refers to the risk which is possible to be exposed under the scope of non-face-to-face transactions, private and correspondent banking services or new products to be offered using developing technologies,

"Simplified Measures" refer to the legislation set forth by the MASAK Communiqué No. 5, which, based on a risk-based approach, allows the measures to be obeyed regarding customer due diligence be applied in a more simplified manner in cases where the risk of money laundering and terrorist financing may be considered low regarding transaction types,

"The Offence of the Financing of Terrorism" refers to providing or collecting funds for a terrorist or terrorist organizations with the intention that they are used or knowing and willing that they are to be used, even without being linked to a specific act, in full or in part, in perpetration of the acts that are set forth as crime within the scope of Article 3 of the Law No. 6415 on the Prevention of Financing of Terrorism,

"UNODC" refers to and stands for the United Nations Office for Drugs and Crime,

"Wolfsberg Principles" refer to all of the principles accepted and treated as an important international guideline for healthy business management in the practices by Banco Santander, Bank of America, MUFG Bank, Barclays, Citigroup, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered and UBS.

SECOND PART
Customer Acceptance

Know Your Customer Principle

Article 4 - Subject to and in accordance with the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism promulgated in the Official Gazette No. 26751 dated January 09, 2008, the Bank has adopted the Know Your Customer principle in all of its transactions with its natural person and legal person customers and all of its corresponding banking relations. To this end, each customer is subject to a preliminary investigation by the relevant bank employees. The purpose here is to ensure openness and transparency in the customer transactions and information, and establishment and maintenance of a relationship based on reciprocal trust.

General Principles in Customer Acceptance

Article 5 - (1) In the Bank, the customer acceptance process is based on and comprised of determination of and collating adequate information about the customer's real identity and address; coherency of the customer's documents and information; the reason of the customer's preference of the bank and the purpose of opening an account; the customer's profession and main revenue- raising activities; profile and capacity of the customer's transactions; suppliers and buyers of the customer; and location of the customer business offices and activities, as well as verifying the accuracy of all such information through other sources.

(2) One of the basic responsibilities of the Bank employees is to investigate not only the financial assets of the customer, but also the sources of his funds and the customer's name and reputation in legal, social and ethical terms.

(3) Customer accounts are opened only in the name of the beneficial owner thereof. At the time of account opening, the customers are requested to give a statement that they are acting and transacting in their own name and account, and not in the account of third persons.

(4) Unless clearly and legally authorized by the customer and proven so by a documentary proof, and unless the account opening purposes and requirements are clarified adequately, demands of third persons to open accounts in the Bank in the name of one or more persons by proxy or under a power of attorney are not accepted and fulfilled.

(5) The Bank avoids entering into customer relationships with persons and organizations, about the illegitimate acquisition of whose material assets has been found or detected a doubt, information or documentary proof upon evaluation and investigation by the Bank.

(6) At the time of account opening, in addition to and other than the basic determination of the customer's identity, all legal, administrative, financial and personal introductory information, i.e. citizenship number, power of attorney, contract, and contact information such as telephone number and electronic mail address, as well as profession and educational background information are requested and taken. Such contact information is confirmed pursuant to and as per the relevant provisions of the regulation.

(7) Information, documents and records on customers are kept up-to-date. The accuracy of the information on telephone and fax numbers and e-mail addresses received for the identification of customers is confirmed upon contacting the relevant person by using these tools when necessary within the framework of a risk-based approach.

(8) In the Bank, all customer relationships are based on continuous communication and reciprocal information exchange and trust and transparency. The Bank neither accepts as its customer nor performs the transactions of the persons and organizations that show reluctance in and refrain from filling in the customer information and introduction forms, fail to submit and file the documents required for customer identification, fail to submit sufficient information on the purpose of the business relationship, or provide misleading or unverifiable information.

(9) It is recommended that enhanced diligence is placed on opening an account for and in the name of exchange offices (authorized institutions); jewelers; traders of precious stones and metals such as gold, etc.; travel agencies; passenger and cargo transporters; casinos; dealers of luxury vehicles; dealers of antiques; art galleries; carpet traders; real estate brokers; leasers of air and sea crafts and vehicles; traders of finished leather goods; producers and traders of auto spare parts; factoring companies; payment and electronic money institutions, crypto asset service providers, producers of arms and military ammunition and cash-based businesses and similar other industries and profession groups generally termed and named as "Risky Sectors and Profession Groups", and also that their customer identity and descriptive documents as well as their industry information are recorded carefully and completely, and that their customer accounts are monitored diligently. Moreover, if and whenever deemed necessary, periodic inspection and audit reports are requested and received from foundations and associations, so as to monitor and follow up their fields of activity or their financial standing.

(10) In the establishment of a business relationship with crypto asset service providers, at a minimum, the following measures shall be applied:

a) Obtaining information, to the extent possible, on the source of the asset subject to transaction and source of funds of the customer,
b) Obtaining information on the reasons for the transaction,
c) Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that needs further examination,

ç) Taking appropriate measures to set limits on the amount and number of transactions,
d) Requiring approval of the next level personnel for the establishment of the business relationship with crypto asset service providers.

(11) The Bank should be cognizant of the sensitivity of organizations and entities managing funds of others such as financial institutions, intermediary institutions, portfolio management companies and investment (mutual) funds shown towards the Prevention of Laundering of Proceeds of Crime, and of the applicable laws and regulations to which they are subject, and of adequacy of their policies and procedures in connection therewith. If and when deemed fit and necessary, the Bank receives and holds an information and statement form or memorandum from its counterparty verifying that the latter shows such diligence and care.

(12) It is preferred not to work or cooperate with persons resident in anti-democratic countries and territories of the world, called "Gray Zones", where the rules of the law system are not practiced, and are along the illegal drug production distribution lines where both the organized crime activities such as smuggling and terrorism, and corruption and bribery are very widespread. However, if and when it is necessary to work or cooperate with such persons, then and in this case, reinforced and enhanced "Know-Your-Customer" principles and approval and monitoring standards are followed up.

(13) Because of higher risks contained therein, certain reinforced and enhanced customer recognition (Know Your Customer), approval and monitoring standards are applied for customers resident in, or for transactions associated with, Offshore Centers and (Offshore) Free Zones which are regarded as attractive centers for depositing of the funds earned from organized crime activities or used in financing of terrorism due to the banking secrecy, tax advantages and legal immunity they offer, or International Finance Centers where strict banking secrecy rules and laws are applied.

(14) The Bank takes necessary measures to determine if a customer or Beneficial Owner is a Politically Exposed Person or not.

Customer Identification and Confirmation

Article 6 - Customer identification must be completed at the time of opening a customer account, and legible photocopies or electronic image of the relevant document shall be received or information regarding the identity shall be recorded. The Bank,

a) Regardless of the amount in the establishment of a permanent business relationship,
b) When the single transaction amount or the total amount of multiple linked transactions is at or above the amount set by the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism,
c) In electronic transfers and crypto asset transfers carried out by crypto asset service providers, when the single transaction amount or the total amount of multiple linked transactions is at or above the amount set by the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism,
ç) Regardless of the amount, when there is suspicion about the adequacy and accuracy of the customer identification information previously obtained,

d) Regardless of the amount, in cases requiring suspicious transaction reporting, determines the identity of its customers and those acting on behalf of or on account of its customers by obtaining information regarding the identity and confirming the accuracy of this information, and takes the necessary measures to reveal the beneficial owner of the transaction. Identification shall be completed before the establishment of a business relationship or before the transaction is carried out. In establishing a permanent business relationship, information shall be obtained about the purpose and nature of the business relationship.

The customer identification methods required to be applied are detailed below.

Customer Identification of Natural Persons

Article 7 - (1) In customer identification of natural persons, their name, surname, date of birth, nationality, type and number of the identity card, address, sample of signature, information on job and profession and telephone number, fax number, e-mail, if any, and for Turkish citizens, as additional information, T.R. identity number, for non-Turkish citizens, the place of birth information shall be received.

(2) The name and surname, date of birth, Republic of Türkiye identity number, and the type and number of the identity document shall be verified through:

a) For Turkish citizens; T.R. identity card, T.R. driver's license or passport, and any identity documents which bear Republic of Türkiye identity number and are clearly specified as official identity documents in their special legislation,
b) For non-Turkish citizens; passport, certificate of residence or any identity document deemed eligible by the Ministry. After originals or notarized copies of identity documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request from authorities.

(3) The address submitted while establishing permanent business relationship shall be verified through a certificate of residence, any utility bill drawn up within the previous three months from the date of transaction for a service requiring subscription such as electricity, water, natural gas, telephone, any document issued by a public institution or through any other documents or methods approved by MASAK. Legible photocopies or electronic image of the documents to be verified shall be received or the information specific to them shall be received.

Remote Customer Identification of Natural Persons and Legal Persons Registered with the Trade Registry

Article 8 - Remote identification methods may be used to verify the identity of the customer in establishing a permanent business relationship with natural persons or legal persons registered with the trade registry, in the event that a contract is established with the customer related to the Bank's primary field of activity by means of methods enabling the verification of the identity of the customer without coming face to face.

Customer Identification of Legal Persons Registered with the Trade Registry

Article 9 - (1) In customer identification of legal persons registered to trade registry, the title of the legal person, its trade registry number, tax identity number, field of activity, full address, telephone number, fax number and e-mail, if any, and the name, surname, date of birth, nationality, type and number of the identity card, and a sample signature of the person authorized to represent the legal person and for Turkish citizens, as additional information, T.R. identity number, for non-Turkish citizens, the place of birth information shall be received.

(2) The title of the legal person, its trade registry number, field of activity, full address shall be verified through documents of registration to the trade registry; its tax identity number shall be verified through documents drawn up by the related unit of Revenue Administration.

(3) Identification information of persons authorized to represent the legal person shall be verified through identity cards stipulated in Article 7 and their authority to represent shall be verified through documents of registration.

(4) After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

(5) In establishing permanent business relationship, the Bank shall verify through consulting records kept by the related trade registry office or the database of Turkish Union of Chambers and Commodity Exchanges whether the information given in registration documents are up-to-date and correct.

(6) In case of a request of transaction, within the scope of an existing permanent business relationship, on behalf of the legal person by a written instruction of the person authorized to represent the legal person the authenticity of the identification information of the person authorized to represent the company may be verified through a notarized signature circular comprising the information in identity cards provided that there is no doubt that the instruction is from the representative of the company.

Customer Identification of Associations and Foundations

Article 10 - (1) In customer identification of associations the name of the association, its aim, log number, tax identification number, full address, telephone number, fax number and e-mail, if any, and the name, surname, date of birth, nationality, type and number of the identity card and sample signature, and for Turkish citizens, as additional information, T.R. identity number, for non-Turkish citizens, the place of birth information of the person authorized to represent the association shall be received. The name, aim, log number and full address of the association shall be verified through the charter of the association and documents of registry in the associations' log; tax identity number shall be verified through documents drawn up by the related unit of Revenue Administration; the identification information of the person authorized to represent the association shall be verified through identity cards stipulated in Article 7; and the authority to represent shall be verified through documents of authorization to represent.

(2) In customer identification of foundations the name of the foundation, its aim, central registry record number, tax identification number, full address, telephone number, fax number and e-mail address, if any, and the name, surname, date of birth, nationality, type and number of the identity card and sample signature of the person authorized to represent the foundation and for Turkish citizens the additional information as T.R. identity number, for non-Turkish citizens, the place of birth information shall be received. Name, central registry record number, full address of the foundation shall be verified through foundation deed and records kept by the General Directorate of Foundations, tax identity number shall be verified through documents drawn up by the related unit of Revenue Administration, the identity information of the person authorized to represent the foundation shall be verified through identity cards stipulated in Article 7; and the authority to represent shall be verified through documents of authorization to represent.

(3) After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

(4) Customer identification for branches and representatives of foreign associations and foundations in Türkiye shall be conducted depending on registry documents at the Ministry of Interior.

Customer Identification of Trade Unions and Confederations

Article 11 - (1) In identification of workers' unions and confederations, information such as name, objectives, registry number, tax identification number, full address, telephone number, fax number (if any) and electronic mail address of the union or confederation, as well as the first name and surname, birth date, nationality of the persons authorized to represent the union or confederation, type and number of identity document and sample of signature, T.R. identity number as for the Turkish citizens, place of birth information for non-Turkish citizens are received and collated. The information collected as above is confirmed through comparison with the internal bylaws of these entities and other registration documentation kept in the provincial labor directorates affiliated to the Ministry of Family, Labor and Social Security; tax identity number shall be verified through documents drawn up by the related unit of Revenue Administration; and identity of the real persons acting for and on behalf of the union or confederation shall be verified through identity cards stipulated in Article 7, while their authorization is confirmed through the said registration documentation or the certificates of authorization granted to them.

(2) After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

Customer Identification of Political Parties

Article 12 - (1) In identification of political party organizations information such as name, full address, telephone number, fax number (if any) and electronic mail address of the relevant unit of the political party, as well as the first name and surname, birth date, nationality type and number of identity

document, sample of signature of the persons authorized to represent the political party, and for Turkish citizens, as additional information, T.R. identity number, for non-Turkish citizens, the place of birth information are received and collated. The information of name and address of the relevant unit of the political party is confirmed through comparison with its internal by laws, and identity of the real persons acting for and on behalf of the political party is determined in accordance with the real person customer identification method, while their authorization is confirmed through the certificates of authorization granted to them.

(2) After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

Customer Identification of Non-Resident Legal Persons and for Trust Agreements Established Abroad

Article 13 - (1) Customer identification of non-resident legal persons shall be made through copies of the documents which correspond to the related country documents required for legal persons residing in Türkiye, are approved by the consulates of the Republic of Türkiye or are attached with an apostille by an authority of a country which is a party to the "Convention Abolishing the Requirement of Legalization for Foreign Public Documents". Furthermore, within a risk- based approach, identity information shall be verified through notarized Turkish translations of copies of these documents when necessary.

(2) In the event that a transaction requiring identification is requested by the natural person of legal person trustee specified in the contract to the account of the asset constituting the subject of a trust agreement established abroad, it shall be declared in writing that the transaction is requested to the account of the asset created under the trust agreement before these transactions are made. Customer identification for trust agreements established abroad shall be made through written copies of the trust agreement which are approved by the consulates of the Republic of Türkiye or are attached with an apostille by an authority of a country which is a party to the "Convention Abolishing the Requirement of Legalization for Foreign Public Documents". Within a risk- based approach, identity information shall be verified through notarized Turkish translations of copies of these documents when necessary. Furthermore, identity information obtained for the identification of the trustee shall be verified in accordance with Article 7 or 9. In determining the beneficial owner, the identity information of the person establishing the contract and of the beneficiary or beneficiary groups as well as the persons designated as auditors, if any, under the contract shall be obtained, and reasonable measures shall be implemented to verify such information. Required measures shall also be taken to reveal the natural person or persons who ultimately control the said assets.

(3) For the purposes of the second paragraph, a trust agreement shall be interpreted as the legal relationship that provides for the transfer of an asset by the person establishing the contract, who is the owner of the asset, to the control of a trustee executing the contract for the management and use of the asset or for other dispositions specified in the contract, all to ensure that a certain beneficiary or a group of beneficiaries benefit the asset in question.

Customer Identification of Unincorporated Organizations

Article 14 - (1) In transactions carried out on behalf of unincorporated organizations such as building, housing estate or office block management, the name of the organization, its full address, telephone number, and fax number and e-mail address, if any, and name, last name, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the organization and for Turkish citizens the additional information as T.R. identity number, for non-Turkish citizens, the place of birth information shall be received. The identity information of the person authorized to represent the organization shall be verified in accordance with the procedure for the identification of natural persons while the information of the organization and the authorization status of the person acting on behalf of the organization shall be verified through the notarized docket.

(2) In customer identification of organizations such as unincorporated joint venture the name of the joint venture, its aim, its full address, telephone number, fax number and e-mail address if any; and name, last name, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the organization and for Turkish citizens, as additional information, T.R identity number, for non-Turkish citizens, the place of birth information shall be received. Information indicating the name, aim, activity field and the address of the partnership shall be verified through notarized partnership agreement; tax identification number shall be verified through the certificates drawn up by the relevant unit of Revenue Administration; identity of persons requesting transaction on behalf of the joint venture shall be verified in accordance with the real person customer identification method; their authorization shall be verified through the documents indicating the authority to represent.

(3) After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

Customer Identification of Public Institutions

Article 15 - In the banking transactions entered into with public administrations in the coverage of general administration, or with professional organizations treated as public administrations, as per and under the Public Fiscal Administration and Control Law No. 5018, identity of the real persons acting for and on behalf of these entities is determined and checked in accordance with the real person customer identification method, while the information about the authorization of the real persons acting for and on behalf of the organization is confirmed through the certificates of authorization issued in accordance with the laws.

Customer Identification of Those Acting on Behalf of Others

Article 16 - (1) In the event that a transaction is requested on behalf of legal persons or unincorporated organizations by persons who are given the authority by the persons authorized to represent;

a) Customer identification of legal persons and unincorporated organizations shall be carried out in accordance with Articles 9 to 14.

b) Customer identification of persons authorized to represent legal persons or unincorporated organizations and the persons who are given the authority by persons authorized to represent shall be carried out in accordance with the procedure in Article 7. In cases where the customer identification of the person authorized to represent cannot be carried out through the identity documents specified in Article 7, the customer identification shall be carried out through power of attorney or circular of signature provided that they contain the information specified in identity documents and that they are notarized.

c) Authorization of persons who are given the authority by the persons authorized to represent shall be verified through notarized proxy or a written instruction of persons authorized to represent. The signatures on the written instruction of persons authorized to represent are verified through their signatures on the notarized circular of signature.

(2) In the event that transactions are made by another person on behalf of a customer that is natural person, customer identification of the person acting on behalf of the customer shall be carried out in accordance with Article 7. Besides, authorization of the person acting on behalf of the customer shall be verified through the notarized power of attorney. In cases where identification of the customer on behalf of whom the act is carried out cannot be conducted in accordance with Article 7, it shall then be conducted through the notarized power of attorney. In the event that the identification of the customer on behalf of whom the act is carried out has already been made due to previous transactions, the requested transaction can be conducted through the written instruction of the customer on behalf of whom the act is carried out provided that the customer's signature on the written instruction is verified through his/her signature which is already available to the Bank.

(3) In transactions carried out on behalf of minors and persons under legal disability by their legal representatives, the authority of those appointed as guardian by court decision, curators and trustees are verified through the original or notarized copy of the relevant court decision. In the event that fathers and mothers request a transaction on behalf of their minor child, it shall be sufficient to identify the child on behalf of whom the transaction is requested and the parent requesting the transaction in accordance with Article 7.

(4) After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

Control of the Authenticity of Documents Subject to Verification

Article 17 - Bank shall verify the authenticity of documents as much as possible by applying to person or institution arranging the document or to other competent authorities in cases where they suspect of the authenticity of documents used for the verification of the information.

Customer Identification in the Subsequent Banking Transactions

Article 18 - In the subsequent face-to-face transactions conducted under permanent business relationship of those who were duly identified formerly, identity data shall be received and compared with the Bank's data. After making comparison, the name and surname of the natural

person who is conducting the transaction shall be entered into the related document and his/her sample signature shall be received. In the event that there is suspicion on the authenticity of the data received, these data shall be verified after the submission of identity documents which are subject to verification or of their notarized copies with the Bank's data. As to the subsequent transactions that require customer identification conducted by using the systems allowing non-face-to-face transactions, necessary measures shall be taken for authentication of the customer and updating the information for customer identification.

Customer Identification of Those Acting for the Benefit of Others

Article 19 - (1) Necessary actions are taken in order to determine whether the applicant is acting for and on behalf of another person or not. To this end, reminder notes as to the responsibility of persons acting in their own name, but in account of other persons are posted at places easily visible by all customers in all Branch Offices and Departments of the Bank serving directly to the customers. The Bank shall also receive, in the establishment of permanent business relationship, the written declaration of the customer indicating whether the act is carried out for the benefit of someone else.

(2) In cases where the person requesting the transaction declares that he/she is acting for the benefit of someone else, the identity and the authority of the person/legal person requesting the transaction and the identity of the person/legal person for the benefit of whom the transaction is conducted shall be identified in accordance with Article 7.

(3) In cases where there is a suspicion that the person is acting in his/her own name but for the benefit of someone else although he/she has declared that he/she is not acting for the benefit of someone else, measures for the identification of the beneficial owner shall be applied.

Identifying the Beneficial Owner

Article 20 - (1) The Bank shall take necessary measures in order to detect the beneficial owner. To this end, the identity information of the identified beneficial owner shall be verified. A notarized circular of signature including identity information can be used for verification.

(2) When establishing permanent business relationship with legal persons registered to trade registry, the Bank shall identify, in accordance with Article 7, the natural or legal person partners holding more than twenty-five percent of the legal person's shares as the beneficial owner. The verification of the identity information required to be obtained within this scope of the legal entity partners residing abroad can be made through open sources containing the official data of the equivalent institutions of the Union of Chambers and Commodity Exchanges of Türkiye in the relevant country.

(3) In cases where there is a suspicion that the natural person partner holding more than twenty-five percent of the legal person's shares is not the beneficial owner or where there is no natural person holding a share at this rate, necessary measures shall be taken in order to detect the natural person(s) who is/are ultimately controlling the legal person. Natural person(s) detected shall be considered as beneficial owner.

(4) In cases where the beneficial owner cannot be detected according to paragraph (2) and (3) above, the natural person(s) registered to trade registry that have the power and authority to represent the legal person at the top-level management shall be considered as beneficial owner.

(5) In a permanent business relationship with other legal persons and unincorporated organizations, necessary measures shall be taken in order to detect the natural person(s) who is/are ultimately controlling the legal person. In case where the beneficial owner cannot be detected, the natural person(s) that have the power and authority to represent the legal person at the top-level management shall be considered as beneficial owner.

THIRD PART
Duties, Powers and Responsibilities

Article 21 - All employees of the Bank at all levels are obliged to implement the relevant processes within the scope of this Policy and the Compliance Program at the Head Office and branches of the Bank in a purposeful and effective manner, and to fulfil all their duties and responsibilities correctly and carefully to prevent the Bank from being exposed to risks related to financial crimes and sanctions. The Board of Directors of the Bank is ultimately responsible for the adequate and effective implementation of the Policy and the Compliance Program as a whole.

Under the Compliance Program, the Board of Directors shall be authorized and responsible;

a) To ensure the Bank's compliance with the obligations related to combating financial crimes,
b) To approve the organization's policies, annual training programs and the amendments thereto,
c) To appoint a Compliance Officer and Assistant Compliance Officer(s),
ç) To approve the duty regulation that regulates the authorities and responsibilities of the Compliance Officer and the compliance unit reporting to the Compliance Officer,
d) To evaluate the results of risk management, monitoring and control and internal audit activities carried out within the scope of the compliance program and to ensure that necessary measures are taken,
e) To ensure that all activities within the scope of the compliance program are carried out effectively and in coordination.

Under the Compliance Program, the Senior Management of the Bank shall be responsible to the Board of Directors for:

a) Establishing business processes and duty regulations in accordance with the Policy within the framework of banking corporate governance principles,
b) Proper and effective implementation of the procedures by all employees,
c) Taking the necessary measures in a timely manner to ensure that the Bank is not exposed to risks related to financial crimes and sanctions.

Appointing Compliance Officer and Assistant Compliance Officer(s)

Article 22 - (1) Pursuant to the relevant article of the Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism promulgated in the Official Gazette No. 26999 dated September 16, 2008, the Bank shall appoint a Compliance Officer at the administrative level who shall directly report to the Board of Directors and meets the conditions set forth in the Regulation.

(2) At least one Assistant Compliance Officer who meets the conditions and qualifications required for the Compliance Officer shall be appointed to execute the Compliance Program. The Assistant Compliance Officer(s), who is appointed for the same term and in the same manner as the Compliance Officer, shall be appointed exclusively as an employee of the Bank reporting to the Compliance Officer.

(3) In the event that the Compliance Officer or Assistant Compliance Officer ceases to fulfil the conditions required pursuant to the Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism or it is subsequently understood that they do not meet these conditions or they leave their position, the Bank shall notify MASAK in writing within ten days following the date of resignation. A new appointment for the Compliance Officer and, if necessary, the Assistant Compliance Officer shall be made within thirty days at the latest from the date of resignation. The commitment form regarding the appointment shall be signed by the Board of Directors or the member or members of the Board of Directors to whom the Board of Directors delegates its authority and be submitted to the MASAK Presidency within ten days from the date of appointment.

(4) Until a new Compliance Officer is reappointed or in case the Compliance Officer temporarily leaves office due to leave, illness or similar reasons, the Assistant Compliance Officer shall act in their stead.

Duties, Powers and Responsibilities of Compliance Officer

Article 23 - (1) The duties and responsibilities of the compliance officer appointed under Article 22 are as follows:

a) To perform the necessary work to ensure compliance with the Law and the regulations issued pursuant to the Law, and to ensure the necessary communication and coordination with the MASAK Presidency,
b) To establish corporate policies and procedures and submit the corporate policies to the Board of Directors for approval,
c) To establish the risk management policy and perform risk management activities,
ç) To establish monitoring and control policies and perform related activities,
d) To submit their work on the training program for the prevention of laundering proceeds of crime and financing of terrorism to the Board of Directors for approval, and to ensure the approved training program is effectively implemented,
e) To investigate, to the extent of reach of his/her powers and within the bounds of possibility, the suspicious or dubious transactions or actions reported to him/her or learned directly by him/her ex

officio, and to evaluate the resulting findings and information, and to report to MASAK Presidency the transactions believed to be suspicious,

f) To take necessary measures to ensure the confidentiality of notifications and other related matters,

g) To keep information and statistics on internal audit and training activities regularly, and to send them to the Presidency within the periods specified in the relevant legislation.

(2) To ensure the necessary communication and coordination with the MASAK Presidency, the obligation to provide information and documents to the Presidency shall be fulfilled through the compliance officer. The requested information and documents shall be provided in the format and by the method determined by the Presidency.

(3) The Compliance Officer shall act in good faith, reasonably and honestly, and with an impartial and independent will while fulfilling their duties and responsibilities.

(4) The Compliance Officer has the authority to make decisions with an independent will, to request all kinds of information and documents related to their purview from all units, and to access them in a timely manner.

FOURTH PART
Principles on Reporting of Suspicious Transactions and Suspicious Transactions with Postponement Request

Suspicious Transactions

Article 24 - Suspicious transaction is the case where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism.

Principles on Reporting Suspicious Transactions

Article 25 - (1) It is a duty and obligation of all Bank employees to recognize, detect and report suspicious transactions or activities.

(2) Suspicious activities and transactions shall be reported to MASAK Presidency regardless of the amount thereof.

(3) When necessary, multiple transactions shall be taken into consideration together in order to determine whether there is suspicion or a reasonable ground to suspect.

(4) Reporting of suspicious activities and transactions as a part of continuous information and reporting obligations shall not eliminate the specific obligation of reporting a suspicious activity and transaction.

(5) In case of any suspicion, the employee shall inform the Compliance Officer about the transaction without delay by filling out the Suspicious Transaction Reporting Form (STRF). Notifications have to be made in accordance with the procedures and principles specified in the guidelines published by MASAK Presidency.

(6) The Compliance Officer shall review and evaluate the information contained in the Suspicious Transaction Reporting Forms sent to him/her by also considering the contents of the relevant applicable laws, regulations and communiques, and depending on the results of evaluation, shall decide to or not to report the underlying transaction as a suspicious activity to MASAK Presidency.

(7) The Compliance Officer shall act in good faith, reasonably and honestly in the course of the decision making process. An STRF with a decision not to report and the written grounds thereof shall be kept and archived for a period of 8 years for submission to the official authorities if and when deemed necessary.

(8) It is obligatory to report the suspicious activities or transactions to MASAK Presidency within 10 workdays starting from the date when the suspicion arose and immediately where any delay is inconvenient.

(9) In the event that new information and findings in relation to the reported transaction are obtained afterwards, another STRF shall be filled in and sent to MASAK Presidency without delay by stating that it is an additional report to the previous one.

(10) Confidentiality is essential in the reporting of suspicious transactions. The Bank shall not disclose any information that the suspicious transaction has been or will be reported to anyone including the parties of the transaction, and the other organizations within the same financial group, except for the information provided for the examiners assigned for supervision of obligations and for the courts during trial.

Principles on Reporting Suspicious Transactions with Postponement Request

Article 26 - (1) If there is any document or serious indication supporting suspicion that the assets which are the subject of a transaction attempted to be conducted or currently going on within or through the Bank are linked with the offence of laundering proceeds of crime or financing of terrorism. Suspicious transaction reports within this scope shall be sent by selecting the "Requested Suspension of Transaction" option in the notification urgency section and be considered as higher risk by the MASAK Presidency.

(2) The indicators specified below can be considered as documents or serious indication supporting suspicion.

a) The transaction which is the subject of an STR with a request of suspension is extraordinary,
b) It is understood after the controls made in various databases or other resources that the person(s) carrying out the transaction is or might be related to the offence,

c) There is a risky situation that if the transaction is completed, then the seizure of the funds or the proceeds of crime thought to be related to financing of terrorism might be prevented or complicated.

(3) The Bank submitting STRs with a request of suspension to MASAK Presidency shall abstain from executing the transaction until the decision on the transaction to be made by the Minister is notified to the Bank by MASAK. Duration of postponement of transactions cannot exceed seven workdays following the submitting date of the STR by the Bank. If the decision on the transaction is not notified within that period, the Bank might execute the transaction.

FIFTH PART
Execution of Decisions on Freezing of Asset

Execution of Decisions on Freezing of Asset

Article 27 - MASAK is responsible for the execution of the decision on freezing of assets made in accordance with the provisions of the Law. The decision to freeze assets shall be notified to the Bank by MASAK using the appropriate technical communication tools to ensure that all accounts, rights and receivables are frozen. The said decisions shall be implemented by the Bank immediately upon receipt of the notification. In terms of the risks of the violation, non-implementation and avoidance of Freezing of Asset decisions, the Bank defines, assesses, monitors and mitigates the risk and applies advanced controls for the implementation of the aforementioned sanctions. If the Bank has any records of assets, it shall perform the required action and notify MASAK with information regarding the frozen assets within seven days from the date of notification. MASAK shall notify the Bank on any decisions repealing a decision to freeze assets. In case of any increase in assets, such increases shall also be subject to the provisions on freezing assets. The permission and authorization to access and dispose on frozen assets and the management of the relevant assets shall be administered pursuant to the relevant regulations of MASAK. The Bank shall take the necessary measures to avoid entering into business relations with persons, institutions or organizations for which a Freezing of Assets decision has been made.

SIXTH PART
Risk Management

Compliance Unit

Article 28 - (1) It is the Compliance Officer's responsibility to define risk levels and determine the risk level of customers, to perform regular reviews in accordance with customers' risk levels, to identify the relevant methodology, and to establish enhanced control procedures by taking into account the case studies or executed transactions.

(2) Risk management activities shall be carried out within the Corporate Compliance Department, which reports directly to the Compliance Officer and is responsible for managing the compliance program within the framework of the relevant legislation and the provisions of this Policy hereby.

(3) Risk monitoring and assessment results shall be reported to the Board of Directors at regular intervals.

Risk Management Activities

Article 29 - Appropriate operational and control rules shall be developed to ensure that risky customers, transactions or services are monitored and controlled, necessary measures are in place to reduce risks, risks are reported to warn the relevant units, the transaction is performed upon the approval of the senior management and is audited when necessary.

Risk management activities include the following work:

a) Developing risk identification, rating, classification and assessment methods based on Customer Risk, Service Risk and Country Risk,
b) Rating and categorizing services, transactions and customers according to risks,
c) Monitoring and controlling risky customers, transactions or services, taking necessary measures to reduce risks and reporting them to warn the relevant units,
ç) Developing appropriate operational and control rules to ensure that the transaction is executed upon approval by line management and is audited when necessary,
d) Checking the consistency and effectiveness of risk identification, assessment, rating and classification methods retrospectively through case studies or executed transactions; re-evaluating and updating them according to the conclusions reached as well as emerging conditions,
e) Monitoring principles, standards and guidelines introduced by the national legislation and international organizations regarding risk subjects, and performing the required improvement work,
f) Reporting risk monitoring and assessment results to the Board of Directors.

Risk Assessment

Article 30 - (1) While determining the risk level of the customer, customer, service/product and country risks shall be considered and assessed holistically. The Bank classifies customers subject to services and transactions in its field of activity as low, medium and high risk customers on the basis of identified risk areas. Accordingly, enhanced measures apply to high-risk customers and transactions.

(2) Countries, customer groups, products and services categorized as high risk shall be determined with a risk-based approach within the framework of the relevant legislation and this Policy hereby.

(3) In the assessment of customer risk, the following criteria shall be taken into consideration as a minimum:

a) The customer's profession and field of activity,
b) Type of establishment and shareholding structure of legal entity customers,
c) The customer's country of citizenship and/or residence and/or operation,
ç) Type and nature of the banking products and services used by the customer,

d) Whether the customer is subject to any judicial process,
e) Whether the customer is a Politically Exposed Person,
f) News about the customer in the media, if any, with negative content.

(4) Under Service Risk,

a) Electronic transfers,
b) Systems that allow non-face-to-face transactions,
c) Products and services based on new and emerging technologies,
ç) Correspondent banking transactions,
d) Business and transactions the beneficial owner of which cannot be fully and clearly identified,
e) Other product, service and transaction types that will be deemed risky by their nature and deemed worthy of special attention within the scope of risk management, monitoring and control activities under the compliance program to be carried out in accordance with international norms, legislation and the provisions of this Policy hereby shall be monitored in the high risk category.

(5) Under Country Risk, countries that are assessed to be high risk according to the following criteria shall be closely monitored:

a) Countries that are assessed as not having adequate regulations and practices in combating financial crimes within the scope of the FATF recommendations,
b) Countries that are assessed as risky within the scope of UNODC reports,
c) Countries that are included in the "Risky Countries" list issued by the Ministry of Treasury and Finance,
ç) Countries that are subject to international sanctions within the framework of UNSC resolutions due to their policies and practices related to Laundering Proceeds of Crime or Financing of Terrorism,
d) Countries that are indicated by the European Union or OFAC to bear a high risk of money laundering,
e) Cross-border centers, free zones and financial centers,
f) Tax havens.

(6) At the beginning of and during the business relationship, customers shall be included in the appropriate risk categories in terms of the nature and scope of their activities and their relations and transactions with the Bank, within the framework of the foregoing basic criteria and other customer-specific information and criteria, if any.

(7) Risk-based control measures developed for customers assessed within the high-risk group shall be implemented.

(8) Cases that require special attention, technological risks, and transactions that are part of relations with risky countries shall be considered, and in order to reduce the risk to be assumed in high-risk situations, enhanced measures set by legislative provisions shall apply in proportion to the identified risk.

Enhanced Measures

Article 31 - As part of its risk-based approach, the Bank shall apply enhanced measures to the transactions below:

a) Complex and unusually large transactions and those transactions which lack apparently reasonable legitimate and economic purposes,
b) Transactions with risky countries,
c) Transactions done through new and emerging technologies,
ç) Deposits, withdrawals and electronic transfers performed through systems allowing non-face-to-face transactions,
d) Transactions which do not fit or unrelated with the customer's financial profile and business activities.

Article 32 - (1) In high-risk situations, the Bank shall apply one or more or all of the following measures in proportion to the identified risk:

a) Obtain additional information about the customer and update identification data of the customer and beneficial owner more regularly,
b) Obtain additional information on the intended nature of the business relationship,
c) Obtain information, to the extent possible, on the source of funds of the customer,
ç) Obtain information on the reasons for the transaction and records this information,
d) Obtain approval of senior management to enter into a business relationship, sustain the business relationship or execute the transaction,
e) Conduct enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by identifying the types of transactions requiring additional controls,
f) When setting a permanent business relationship, request the first financial transaction to be carried out through another financial institution that applies customer due diligence principles,
g) Take appropriate and effective measures including setting limits on the amount and number of transactions.

(2) In the business relations established and transactions conducted with Politically Exposed Persons who are elected or appointed by a foreign country or their spouses, first-degree relatives and close associates, the following measures shall apply:

a) To require approval of the next level personnel for establishing a business relationship, sustaining current business relationships or carrying out transactions,
b) To take reasonable measures to determine the source of assets and funds that belong to these persons or are subject to transaction,
c) To conduct enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the types of transactions requiring additional controls.

(3) These measures shall apply to Politically Exposed Persons who are elected or appointed by Türkiye or who work for international organizations or their spouses, first-degree relatives and close associates in case the business relations and transactions with them are deemed high risk.

(4) Close associates of Politically Exposed Persons mean people who have all kinds of social, cultural or economic affinity, which can be considered as a unity of interests or purposes, such as kinship other than first degree, being engaged, company partnership or being a company employee.

(5) In the event that Politically Exposed Persons resign from office or lose their qualifications, the implementation of the measures specified in paragraph two shall continue for at least one year from the date of their resignation or loss of these qualifications. This period may be extended if the transactions or business relations with these persons pose a risk.

Sanctions

Article 33 - (1) The Bank continuously monitors both national and international laws and regulations and the sanctions imposed for the prevention of laundering proceeds of crime, financing of terrorism and proliferation of weapons of mass destruction as well as the lists published within this scope and carries out advanced systematic controls for the implementation of the sanctions in force.

(2) It oversees full compliance, as a minimum, with the sanctions announced by the following countries, institutions and organizations due to financial crimes, corruption or terrorism, including but not limited to the national lists published within the scope of Laws No. 6415 and 7262:

a) United Nations Security Council (UNSC),
b) European Union,
c) United States of America,
ç) United Kingdom

(3) The Bank shall not deliberately become a party to any transaction aimed at circumventing sanctions.

(4) The Bank shall observe sanction risks while accepting new customers, updating customer information and performing customer transactions. To this end,

a) Customers, shareholders, persons acting on behalf of or on account of the customer and beneficial owners are screened through the lists.
b) The Bank examines whether the customer's transactions with or through the Bank directly or indirectly involve a sanctioned Country/Region or a sanctioned person or entity.
c) Customer acceptance does not take place and the transaction is not performed until the evaluations on screening results are completed by the persons authorized for such work.
ç) Regular screenings shall be performed on whether existing customers are included in these lists.

SEVENTH PART
Monitoring, Control and Internal Audit

Monitoring and Control Activities

Article 34 - (1) Monitoring and control activities shall be performed by the Corporate Compliance Department, which reports to the Board of Directors, under the supervision of the Compliance Officer.

(2) The main purpose of monitoring and control is to protect the Bank from risks and to continuously monitor and control the execution of its activities within the framework of the applicable legislation, policies and procedures.

(3) Monitoring and control shall be established and performed with a risk-based approach. In this framework, monitoring and control methods fitting the nature and level of risks associated with the Bank's customers, transactions and services shall be developed and effectively implemented.

(4) The monitoring and control activities performed include at least the following:

a) Monitoring and control of the customers and transactions categorized as highly risky,
b) Monitoring and control of the transactions executed with risky countries and territories,
c) Monitoring and control of complex and unusual transactions,
ç) Checking and testing by sampling method of whether the transactions in excess of a certain threshold amount to be determined in line with the current risk policies are coherent and congruous with the customer profile,
d) Monitoring and control of associated and related transactions which, when taken together, exceed a certain threshold amount that requires identification of customer,
e) Control of the information and documents required to be kept in writing or on electronic medium and of the information required to be given in electronic fund transfer messages about the customer, and requesting the completion of deficiencies, if any, and updating the same if and when required,
f) During the business relationship, ongoing monitoring whether the transaction conducted by the customer is consistent with information regarding business, risk profile and fund resources of the customer,
g) Monitoring of transactions conducted outside the permanent business relationship with a risk-based approach,
ğ) Control of the transactions carried out through using systems enabling the performance of non-face-to-face transactions,
h) Risk-focused control of the banking services which may become exposed to fraud due to recently-introduced banking products and technologic innovations and advancements.

(5) Central monitoring and control activities shall be carried out systematically within the Corporate Compliance Department. On-site audit and control of the effectiveness of the practices and the compliance of the transactions related to the execution of the Compliance Program in the Head Office Departments and branches of the Bank pursuant to the applicable legislation, policies and processes shall be ensured within the scope of internal audit and internal control activities.

(6) Measures shall be taken to continuously monitor customers and transactions, taking into account Freezing of Asset decisions and potential matching criteria. In this context, the sender and receiver information in electronic transfer messages are also considered. In accordance with the Law on the Prevention of the Financing of Terrorism and the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction, persons, institutions or organizations whose Assets are frozen and who have Assets in the Bank are monitored and if there is any increase in the frozen Assets, these increases are also subject to the Freezing of Asset provisions and reported to MASAK Presidency within the timeframes specified by the law.

Internal Audit

Article 35 - (1) The Board of Internal Auditors reporting to the Board of Directors shall carry out its audit and supervision activities so as to inspect, supervise and check on yearly basis and with a risk-based approach whether the Bank's applicable policies and procedures and its risk management, monitoring and control activities and training activities are adequate and efficient or not, and whether the Bank's risk policy is adequate and efficient or not, and whether the transactions are effected and executed in compliance with the Law and the regulations and communiques associated thereto and issued thereunder and the Bank's internal policies and procedures or not.

(2) Deficiencies, faults, errors and frauds detected as a result of internal audit are reported to the board of directors, together with comments and suggestions on prevention of recurrence or repetition of them.

(3) The deficiencies and problems detected in the course of monitoring and control activities and initiatives, as well as the risky customers, services and transactions are all included in the scope of audit.

(4) The units, divisions and transactions to be audited shall be determined by considering the Bank's operational size and transaction volume. Accordingly, the intention will be to audit a sufficient number of units, divisions and transactions of adequate qualifications representing all of the transactions executed by the Bank.

(5) Regarding the activities performed as part of internal audit activity, statistics including information on annual transaction volume, total number of personnel and total number of branches, agencies and similar affiliated units, number of audited branches, agencies and similar units, dates of audits performed in these units, total audit period, personnel employed in the audit and number of audited transactions are reported to the Presidency by the Compliance Officer within the periods stipulated in the legislation.

EIGHTH PART
Information Sharing within the Financial Group

Scope of Information Sharing within the Financial Group and the Sharing Principles

Article 36 - (1) Financial institutions affiliated to Türkiye İş Bankası A.Ş. Financial Group may share information within the group regarding customer identification and accounts and transactions in order to ensure that the measures within the scope of the compliance program are taken at the financial group level. Confidentiality provisions stipulated in special laws shall not apply to intra-group information sharing.

(2) Those working in the Bank may not disclose the information they have learnt within the scope of intra-group information sharing and may not use it for their own benefit or the third parties' benefit. To this end, legal and administrative sanctions shall be imposed on those who disclose confidential information.

(3) The Board of Directors of Türkiye İş Bankası A.Ş., together with the compliance officer of Türkiye İş Bankası A.Ş., shall be responsible for taking the necessary measures for the secure sharing of information within the Financial Group. This responsibility shall also apply to the compliance officer and the Board of Directors of the Bank under the Financial Group.

(4) The compliance officer of the Bank cannot share information within the financial group to reveal that a suspicious transaction has been reported.

NINTH PART
Principles for the Provision of Information and Documents

Periodically Reporting

Article 37 - If demanded so, the Bank is under obligation to report to MASAK any and all transactions to which it is a party or is involved in as the intermediary which are in excess of a threshold amount determined by the Ministry of Treasury and Finance.

Providing Information and Documents

Article 38 - When requested by MASAK or examiners, the Bank is under obligation to provide fully and accurately all kinds of information, documents and related records in every type of environment, any kind of information and passwords necessary for accessing to or making these records decipherable and to render the necessary convenience.

Retaining and Submitting Obligations

Article 39 - (1) The Bank shall retain for eight years, the documents, in all forms, regarding their transactions and obligations starting from the drawn-up date, books and records from the last record

date, identification documents from the last transaction date and submit them when requested. The starting date of retaining period relating to documents on customer identification concerning the accounts is the date when the account has been closed.

(2) Documents and records of suspicious transactions reports made to MASAK Presidency or internal reports made to the compliance officer, documents attached to reports, the written reasons relating to suspicious transactions decided not to be reported by compliance officer, are all in the scope of obligation of retaining and submitting.

TENTH PART
Training

Training Activities

Article 40 - (1) With a view to ensuring and assuring compliance with the obligations and liabilities arising out of the Law and relevant regulations and communiques, and forming and establishing a corporate culture by enhancing and improving the consciousness of the personnel about their liabilities and responsibilities relating to the corporate policies and internal regulations and on risk-based approach, and keeping the personnel informed and aware about the developments, the Corporate Compliance Department and the Human Resources Department shall organize the required training courses and programs and ensure participation of all of the relevant personnel thereto.

(2) The Human Resources Department is responsible for carrying out the necessary organizational work to organize at least one online and/or in-class training with wide participation every year.

(3) To ensure that training activities are disseminated throughout the Bank, seminars and panels can be organized as well as computer-aided online trainings over the internet or intranet.

(4) From a risk-based perspective, trainings shall be of a sufficient duration allowing a complete and understandable instruction to improve employee awareness levels.

(5) Internal/external trainers who are experts in their fields, possess the necessary professional knowledge and experience and have strong references shall be duly selected.

(6) All relevant bank employees (expert staff), including senior management in line with their duties and responsibilities, primarily sales and marketing teams having direct contact with customers as well as support and operation teams, and control and audit teams shall be required to attend the trainings at least once a year.

(7) Training Programs shall be prepared and arranged so as to cover the following as a minimum:

a) Concepts of laundering proceeds of crime and financing of terrorism,
b) Stages and methods of laundering proceeds of crime, and case studies thereon,

c) Laws and regulations pertaining to prevention of laundering proceeds of crime and financing of terrorism,
ç) Risk areas,
d) Corporate policies and procedures,
e) Within the framework of the Law and other associated regulations:
-Principles as to know-your-customer,
-Principles as to reporting of suspicious activities and transactions,
-Safekeeping and submission obligations,
-Obligation to give and disclose information and documents,
-Sanctions applicable in case of breach of these obligations
f) International arrangements and regulations on combating the laundering of proceeds of crime and the financing of terrorism

(8) At the end of the trainings, an evaluation exam is carried out for measurement and evaluation purposes. The personnel failing the end-of-training evaluation exam shall be required to re-take the exam and, if necessary, re-attend the relevant training.

(9) Training activities shall be conducted under supervision and coordination of the Compliance Officer.

(10) Training programs shall be continuously reviewed and revised according to needs and with the participation of relevant units, and they shall be repeated annually so as to keep all relevant Bank personnel updated in line with their duties, obligations and liabilities.

Reporting of Training Results

Article 41 - Regarding the implemented training activity,

a) Training dates,
b) Regions or provinces where training is provided,
c) Training method,
ç) Total hours of training,
d) Number of personnel trained, and the ratio of this number to the total number of personnel,
e) Breakdown of the trained personnel by their units and titles,
f) Content of the training,
g) Information and statistics on the title and specialty of trainers shall be notified to the MASAK Presidency through the Compliance Officer within the periods stipulated in the legislation.

ELEVENTH PART
Special Conditions

Article 42 - (1) The Bank has agreed and undertaken to comply with the Wolfsberg Principles in its practices and transactions.

(2) The Bank pays utmost attention not to accept individual and corporate customers sanctioned and published on the OFAC, European Union (EU), United Nations (UN), United Kingdom (UK) and French sanctions lists as well as the lists published by Public Institutions on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism. It does not act as an intermediary in transactions to which such individuals and organizations are directly or indirectly party. Regular screenings shall be made on whether customers, those acting on behalf of or in the name of customers as well as beneficial owners and their partners are included in the relevant lists. If such links are detected during an existing customer relationship, banking transactions shall be terminated.

(3) The Bank does not mediate prohibited transactions and activities subject to the resolutions of the United Nations Security Council on the prevention of proliferation of weapons of mass destruction and its financing. It acts in accordance with the legislation in the implementation of prohibited transactions and activities in addition to decisions on freezing assets.

(4) The Bank in no event accepts the opening of any account unnamed/anonymous or with fictitious names or in the name of any person other than its real known holder.

(5) In the event that the required identification and verification cannot be made due to doubts about the adequacy and accuracy of the previously obtained customer identification information, the business relationship shall be terminated. Whether the specified situations are suspicious transactions or not shall be evaluated separately.

(6) The Bank pays utmost attention in accepting only customers the origin of whose wealth and funds can be reasonably determined. The attention or diligence required to be shown here is comprised of obtaining from the prospective customer and reviewing and verifying before the account is opened all of the data and information such as purpose of account opening, expected account activities, source of wealth, estimated net worth, source of funds and if any, references for validation of commercial prestige and reputation. The primary responsibility herein is borne by the Bank employee who brings in the customer to our Bank.

(7) Customers established or residing in highly risky countries and offshore territories and those working in highly risky fields of business and civil servants and governmental officers of every hierarchical level and their relatives are also the customers required to be handled carefully.

(8) The Bank pays utmost attention not to accept any customer established or residing in Non-Cooperative Countries and Territories (NCCT) list issued and published by FATF.

(9) The Bank does not accept as customer, or to act as intermediary even in indirect transactions of, banks and companies (shell bank or shell company) which do not have any physical existence or address in any country and at least one employee working on full-time basis and are not subject to the audit of any official authority regarding its banking transactions and records.

Electronic Transfers

(10) In money transfers made through the Bank within the limits set forth in the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, the Bank includes and verifies the following information on the sender:

a) Full name, the title of the legal entity registered with the trade registry, the full name of other legal entities and unincorporated entities,
b) Account number, and reference number related to the transaction in case the account number is not available,
c) Any of the following sender identification information as a minimum: address or place and date of birth or customer number, identity number, passport number, or tax identity number.

In electronic transfer messages, information on the recipient as specified in clauses (a) and (b) of this paragraph shall also be included. Verification of such information is not obligatory.

(11) In domestic and international electronic transfer messages below the limit specified in the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, the information specified in clauses (a) and (b) regarding the sender and recipient shall be included. Verification of such information is not obligatory.

(12) Any incoming money transfer that does not contain the information in clauses (a), (b) and (c) of paragraph 10 above shall be returned or the missing information shall be completed via the financial institution that sent this message.

(13) If the messages sent constantly contain incomplete information and such information is not completed when requested, the Bank shall consider rejecting money transfers from the sending financial institution or limiting transactions or terminating the business relationship with the said financial institution. No transfers shall take place to Anonymous Accounts.

(14) In electronic transfer messages, special attention shall be paid to ensure that the required information regarding the sender is included in the message chain from the financial institution where the order is placed to the financial institution that will make the payment.

Correspondent Relationship

(15) In foreign correspondent relationships, the Bank shall take the following measures:

a) Obtain, by making use of publicly available resources, reliable information on whether the respondent financial institution has been subject to a money laundering and terrorist financing investigation and been punished or warned, its business field, reputation and the adequacy of supervision on it,
b) Assess anti-money laundering and terrorist financing system of the respondent financial institution and ascertain that the system is appropriate and effective,

c) Obtain the approval of the senior manager before establishing new correspondent relationships and documenting the responsibilities of each organization separately,
ç) Ensure that, with regard to correspondent accounts, the customer identity information is confirmed by the bank, that "attention" clause regarding the customers who have direct access to the accounts of the correspondent bank is fulfilled, sufficient Know Your Customer measures are taken, and identity information of the related customer can be submitted to the correspondent bank upon request.

(16) For this purpose, the Bank may, in its sole discretion and if deemed fit and necessary, introduce specific customer acceptance rules, including but not limited to requesting from other financial institutions applying to open correspondent account in the bank, a survey form containing the above given information in writing, and implement specific workflows for which the senior executives' approval is required.

(17) A correspondent relationship shall not be entered into with shell banks and with those financial institutions that lack clearance for not making their accounts available to shell banks.

Reliance on Third Parties

(18) The Bank may enter into business relations or be involved in transactions with customers by relying upon the measures and actions taken by another financial institution in respect of determination of identity of the customer and any person acting for and on behalf of the customer and any real user or beneficiary thereof, and in collection of information about the motives underlying the business relation or transaction as the case may be. However, the Bank assumes final responsibility therein.

(19) Reliance on third parties is possible only if it is ensured that:

a) The third parties have taken other measures which will meet the requirements of customer identification, record keeping and the principles of customer due diligence, and are also subject to regulations and supervision in combating Money Laundering and Financing of Terrorism in accordance with international standards if the third parties are resident abroad,
b) The certified copies of documents (if the permanent business relationship is established through remote identification by the institution that is relied on, the images obtained in the digital environment) relating to customer identification shall immediately be provided from the third party when requested,
c) The identity verification of the customer, whose information is shared, is not carried out by the third party under Simplified Measures.

(20) The principle of reliance on third parties shall not apply if the third party resides in risky countries.

(21) In transactions between financial institutions or where the customer is a public administration or a public professional organization or where the customer is a publicly traded company with its shares listed on the stock exchange, the Bank may apply simplified measures in terms of Know Your Customer requirements as set forth in the General Communiqué (No: 5) of the Financial Crimes Investigation

Board. However, in cases where a risk of money laundering or financing of terrorism may arise, the Bank does not apply simplified measures and acts on the assumption that the transaction may be suspicious.

TWELFTH PART
Enforcement and Update

Article 43 - This policy hereby shall enter into force on the date it is approved by the Board of Directors.

Article 44 - The Policy shall be reviewed by the Corporate Compliance Department under the supervision and coordination of the Compliance Officer at least once a year or as and when required, and if necessary, updates shall be made and submitted to the approval of the Board of Directors.

Article 45 - The policy document and the procedures drafted in relation thereto shall be announced to the relevant Bank employees through information systems and be kept available for the use of the relevant employees at all times.