

**TÜRKİYE SİNAİ KALKINMA BANKASI A.Ş.**  
**INTERNAL REGULATION ON**  
**THE PREVENTION OF LAUNDERING PROCEEDS OF CRIME, FINANCING OF TERRORISM AND**  
**PROLIFERATION FINANCE**

**FIRST PART**

**Purposes, Legal Grounds and Definitions**

**Purposes and Legal Grounds:**

**Article 1:** This Regulation has been prepared and issued for the purpose of guiding the practices of the Bank pursuant to and in line with the pertinent provisions of the articles currently valid and in force of the Law on Prevention of Laundering Proceeds of Crime no. 5549 promulgated in the Official Gazette issue 26323 on 18/10/2006, and the regulations and directives associated thereto, the Law on the Prevention of the Financing of Terrorism no. 6415 promulgated in the Official Gazette issue 28561 on 16/02/2013 and the regulations and directives associated thereto, the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction no. 7262 promulgated in the Official Gazette issue 31351 on 31/12/2020 and the regulations and directives associated thereto, and 40 Recommendations of FATF determining the International Regulations pertaining thereto, and Wolfsberg Principles, and the "Guideline For the Turkish Banking System on Significance of Fight Against Laundering of Crime Revenues and Financing of Terrorism" of the Banks Association of Turkey.

**Abbreviations and Definitions:**

**Article 2:** For the purposes and in the context of this Regulation:

"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 and stands for Türkiye Sınai Kalkınma Bankası A.Ş.;

"Beneficial owner" means natural person(s) who ultimately control(s) or own(s) natural person 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.;

"Proceeds of Crime" means proceeds derived from crime;

"Compliance Officer" refers to the officer who is employed for the purpose of ensuring the compliance with obligations established through the Law or the legislation issued on the basis of the Law and who is entrusted with the required authority;

"Country Risk" means 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 are announced by the Ministry out of those lacking 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” means the risk for obliged parties 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 Tax Inspectors, Treasury and Finance Experts who employed in 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 Turkey;

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

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

“The Offence of the Financing of Terrorism” means providing or collecting funds for a terrorist or terrorist organisations 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;

"Freezing of asset" means 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” means, money or any instruments such as bank credits, bank or travellers cheque, 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;

“Service Risk” means 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;

"Laundering of Crime Revenues" (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;

"MASAK" refers to and stands for the Financial Crimes Investigation Board affiliated to the Ministry of Treasury and Finance;

“Ministry” refers to the Ministry of Treasury and Finance;

"Permanent Business Relationship" means 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;

“Prevention of the Financing of the Proliferation of Weapons of Mass Destruction” refers to sanction decisions of the United Nations Security Council (UNSC) on the prevention of financing the proliferation of weapons of mass destruction;

“Senior Management” refers to the Bank's Chief Executive Officer and Executive Vice Presidents;

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

"Wolfsberg Principles" refers to all of the principles accepted and treated as an important international guideline for healthy business management in the Private Banking practices by ABN AMRO, Banco Santander Central Hispano, Bank of Tokyo - Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Societe Generale, and UBS.

## **SECOND PART**

### **Customer Acceptance**

#### **Know Your Customer Principle:**

**Article 3:** Subject to and in accordance with the "Regulations on Prevention of Laundering Proceeds of Crime and Financing of Terrorism" promulgated in the Official Gazette issue 26751 on 09/01/2008, the Bank has adapted the "Know Your Customer" principle in all of its transactions with its retail, 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 4: (a)** 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.

(b) 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.

(c) Customer accounts are opened only in the name of the real beneficiary and user 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.

(d) 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.

(e) 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.

(f) 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.

(g) In the Bank, all customer relationships are based on continuous communication and reciprocal information exchange and trust and transparency. The Bank does not accept as its customer the persons and organizations that show reluctance in and refrain from filling in the customer information and introduction forms, or fail to submit and file the documents required for customer identification, or provide misleading or unverifiable information.

(h) 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.; non-resident persons; 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, 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.

(i) 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.

(j) 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.

(k) 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.

#### **Customer Identification and Confirmation:**

**Article 5:** 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 customer identification methods required to be applied are detailed below in the following paragraphs.

#### **(a) Customer identification of natural persons**

(1) In customer identification of natural persons, their name, surname, place and 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, the names of mother and father and T.R. identity number shall be received.

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

i) For Turkish citizens; T.R. identity card, T.R. driver's license or passport, and any identity documents which bear Republic of Turkey identity number and are clearly specified as official identity documents in their special legislation,

ii) For non-Turkish citizens; passport, certificate of residence or any type of identity card considered proper by the Ministry. 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.

(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.

#### **(b) Customer identification of legal persons registered to trade registry**

(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, place and 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, the names of mother and father and T.R. identity number 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 5(a) 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.

#### **(c) Customer identification of associations and foundations**

(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, place and date of birth, nationality, type and number of the identity card and sample signature, and for Turkish citizens, as additional information, the names of mother and father and T.R. identity number 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 5(a); 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, place and date of birth, names of mother and father, 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 the names of mother and father and T.R. identity number 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 5(a); 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 Turkey shall be conducted depending on registry documents in the Ministry of Interior.

**(d) Customer identification of trade unions and confederations**

(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 place and date, mother's name, father's name and nationality of the persons authorized to represent the union or confederation, and T.R. identity number, and type and number of identity document as for the 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 is determined in accordance with the real person customer identification method, 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.

**(e) Customer identification of political parties**

(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 place and 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, the names of mother and father and T.R. identity number 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 bylaws, 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 the 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.

**(f) Customer identification of non-resident legal persons and identification of trust agreements established abroad**

(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 Turkey, are approved by the consulates of the Republic of Turkey 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 Turkey

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 5(a) or 5(b). 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.

#### **(g) Customer identification of unincorporated organizations**

(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, place and 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 the names of mother and father and T.R. identity number shall be received. The identity information of the person authorized to represent the organization shall be verified through the identity documents stipulated in Article 5(a); and the organization information and the authorization of the person acting on behalf of the organization shall be verified through notarized docket.

(2) The accuracy of identity information of the real persons acting for and on behalf of the organization is determined and checked in accordance with the real person customer identification method, while the information about the organization and the authorization of the real persons acting for and on behalf of the organization are confirmed through the notary-certified decision book of the organization. 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 through identity documents stipulated in Article 5(a), authorization shall be verified through the documents indicating the authority to represent.

(3) After the 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.

#### **(h) Customer identification of public institutions**

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.

#### **(i) Customer identification of those acting on behalf of others**

(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;

i) Customer identification of legal persons and unincorporated organizations shall be carried out in accordance with Articles 5(b) to (g)

ii) 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 5(a). In cases where the customer identification of the person authorized to represent cannot be

carried out through the identity documents specified in Article 5(a), 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.

iii) 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 5(a). 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 5(a), 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 5(a).

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

### **Customer identification in the subsequent banking transactions**

**Article 6:** In the subsequent banking transactions that require customer identification and effected as a part of continuous business relationship with customers who have already been identified in accordance with the established procedures, only identity information is received and is then compared to the information kept in the bank. In the case of suspicion about accuracy of the information received, the accuracy of such information is checked through comparison of the information held by the bank with the information contained in the confirmatory identity documents or their notary-certified copies after submission and filing of the latter.

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 7:** (a) Necessary actions are taken in order to determine whether the applicant is acting for and on behalf of another person or not, and the identity of the real user and beneficiary of the intended transaction. 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.

(b) 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 5(a).

(c) 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.

### **Identification of Beneficial Owner**

**Article 8:** (a) The Bank shall take necessary measures in order to detect the beneficial owner. The identification documents shall be verified. A notarized circular of signature including identity information can be used in this respect.

(b) When establishing permanent business relationship with legal persons registered to trade registry, the Bank shall identify, in accordance with Article 5, the natural or legal person partners holding more than twenty-five percent of the legal person's shares as the beneficial owner. The confirmation 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 Turkey in the relevant country.

(c) 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. And natural person(s) detected shall be considered as beneficial owner.

(d) In cases where the beneficial owner can not be detected according to paragraph (b) and (c), 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.

(e) 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 can not 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**

### **Appointment of Compliance Officer, Powers, Duties and Responsibilities of Compliance Officer**

#### **Appointment of Compliance Officer:**

**Article 9:** Pursuant to the provisions of Article 4 of the Regulation on Actions and Measures, and Article 29 of the Regulation on Compliance Program for Prevention of Laundering Proceeds of Crime and Financing of Terrorism promulgated in the Official Gazette issue 26999 on 16/09/2008, the Bank appoints an exclusive Compliance Officer bearing and satisfying the qualifications sought for in Article 30 thereof, who will administratively report directly to the Board of Directors. The decision relating to the assignment shall be drawn up as written in order to submit when requested by authorities. Assignment of deputy compliance officer shall be carried out in accordance with Article 32 of the of the Regulation on Compliance Program for Prevention of Laundering Proceeds of Crime and Financing of Terrorism. Bank branches established abroad are to assign "Compliance Officers" which will be responsible toward the official authorities and governmental bodies of the country.

## **Powers, Duties and Responsibilities of Compliance Officer:**

**Article 10:** (a) To investigate, to the extent of reach of his powers and within the bounds of possibility, the suspicious or dubious transactions or actions reported to him or learned directly by him ex officio, and to evaluate the resulting findings and information, and to report to MASAK (The Financial Crimes Investigation Board) the transactions believed to be suspicious;

(b) To act in good faith, reasonably and honestly, neutrally and with his own free will and volition in reviewing and evaluating the suspicious transactions and in reporting them to MASAK, and to take all required actions for confidentiality of such reports and disclosures;

(c) To request all kinds of information and documents from all and any units and organs of the Bank as and to the extent required in the course of evaluation and review of suspicious transactions and

(d) To conduct and manage the training, research, development, supervision, risk management by taking into account the risks identified within the scope of the national risk assessment monitoring, oversight and control activities and to assure the required coordination and communication with MASAK with a view to ensuring compliance of the Bank with all its obligations arising out of the relevant laws, regulations and communiques.

## **FOURTH PART**

### **Reporting of Suspicious Transactions and Suspicious Transactions with Postponement Request**

#### **Suspicious Transactions:**

**Article 11:** 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.

#### **Principals of Reporting Suspicious Transactions:**

**Article 12:** (a) It is a duty and obligation of all Bank employees to recognize, detect and report suspicious transactions or activities.

(b) Suspicious activities and transactions are reported to MASAK, regardless of the amount thereof.

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

(d) Reporting of suspicious activities and transactions as a part of continuous information and reporting obligations does not eliminate or abolish the specific obligation of reporting of a certain suspicious activity and transaction.

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

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

(g) The Compliance Officer will act in good faith, reasonably and honestly in the course of decision making process. The Suspicious Transaction Reporting Forms decided not to be reported and transmitted will, together with the written grounds thereof, be kept and archived for a period of 8 years for submission to the official authorities if and when requested or deemed necessary.

(h) It is obligatory to report the suspicious activities or transactions to MASAK within 10 (ten) workdays starting from the date when the suspicion occurred.

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

(j) 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 organisations within the same financial group, except for the information provided for the examiners assigned for supervision of obligations and for the courts during trial.

#### **Principals of Reporting Suspicious Transactions with Postponement Request:**

**Article 13:** 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 is linked to offence of laundering or financing of terrorism, the Bank shall submit a suspicious transaction report (STR) to MASAK with their grounds including the request of suspension of the transaction.

The indicators specified below can be considered as documents supporting the suspicion or serious indication;

- (a) If the transaction which is the subject of a STR with a request of suspension has an extraordinary qualification,
- (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 seizure of the funds or the proceeds of crime thought to be related to financing of terrorism might be prevented or complicated.

The Bank submitting STRs with the request of suspension to MASAK shall abstain from execution of the transaction until the decision on the transaction to be made by the Minister is notified to them by MASAK. Duration of postponement of transactions cannot exceed seven work days 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 14:** MASAK is responsible for the execution of the decision on freezing of asset 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. 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 also notify the repealing decisions to the persons, organisations and institutions that's assets have been frozen. 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.

### **SIXTH PART**

#### **Risk Management**

**Madde 15 –** Appropriate operational and control rules are 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. As part of risk management activities, the recommendations, principles, standards and guidelines introduced by the national legislation and international organizations regarding risk subjects shall be followed up, and the required improvement work shall be carried out. While determining the risk level of the customer, customer, service/product and country risks shall be considered and assessed holistically. The Bank classifies customers 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.

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. Risk-based controls shall be implemented for high-risk customers.

The Bank shall take enhanced measures for the below detailed transactions:

- Complex and unusual large transactions and the ones which have no apparent reasonable legitimate and economic purpose
- Transactions done with risky countries
- Transactions done through new and developing technologies
- Non face-to-face wire transfer transactions
- Transactions which are not suitable with the customers economic situation and business activities.

### **Enhanced Measures**

- Obtain additional information about the customer and update identification data of the customer and beneficial owner more regularly,
- Obtain additional information on the intended nature of the business relationship,
- Obtain information, to the extent possible, the source of funds of the customer,
- Obtain information on the reasons for the transaction,
- Obtain approval of senior management to continue the business relationship or carry out the transaction,
- Increase the number and frequency of the controls
- 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.

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.

## **SEVENTH PART**

### **Monitoring, Control and Internal Audit**

#### **Monitoring and Control Activities:**

**Article 16:** Monitoring and control activities are performed by the Internal Control Department under the supervision of the Compliance Officer.

The scope of monitoring and control activities performed is detailed below.

- (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;
- (d) 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 or not;

- (e) Monitoring and control of associated and related transactions which, when taken together, exceed a certain threshold amount that requires identification of customer;
- (f) Control of the information and documents required to be kept in writing or in 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;
- (g) 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
- (h) Control of the transactions carried out through using systems enabling the performance of non face-to-face transactions,
- (i) Risk-focused control of the banking services which may become exposed to fraud due to newly introduced banking products and technologic innovations and advancements.

#### **Internal Audit:**

**Article 17:** The Board of Internal Auditors will 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 there under and the Bank's internal policies and procedures or not.

- (a) 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.
- (b) 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.
- (c) The units, divisions and transactions to be audited will 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.

### **EIGHTH PART**

#### **Periodic Reporting, Providing Information and Documents, Retaining and Submitting Obligations**

##### **Periodic Reporting Obligations:**

**Article 18:** The Bank is under obligation to report to MASAK all and any 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 if demanded so.

##### **Providing information and documents:**

**Madde 19:** 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 render necessary convenience.

##### **Retaining and Submitting Obligations:**

**Article 20:** (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 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.

## **NINTH PART**

### **Training**

**Article 21:** 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 issues, and keeping the personnel informed and aware about the developments, the Internal Control Department and the Human Resources Department will organize the required training courses and programs and ensure participation of all of the relevant personnel thereto.

Training Programs will be prepared and arranged so as to cover the following points and issues at minimum:

- (a) Concepts of laundering of crime revenues and financing of terrorism;
- (b) Stages and methods of laundering of crime revenues and proceeds, and case studies thereon;
- (c) Laws and regulations pertaining to prevention of laundering of crime revenues and financing of terrorism;
- (d) Risk areas;
- (e) Corporate policies and procedures;
- (f) Within the frame 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 and
  - Sanctions applicable in case of breach of these obligations;
- (g) Training activities about international arrangements and regulations on combat against laundering and financing of terrorism will be conducted under supervision and coordination of the Compliance Officer. Training programs will be continuously reviewed and revised according to the current needs, and will be repeated annually so as to keep the knowledge of all relevant Bank personnel updated in line with their duties, obligations and liabilities.

## **TENTH PART**

### **Special Conditions**

**Article 22:**

- (a) The Bank has agreed and undertaken to comply with Wolfsberg Principles in its practices and transactions.
- (b) 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.
- (c) 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.
- (d) 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.

- (e) Furthermore, 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.
- (f) Politically Exposed Persons (PEPs): According to the FATF terminology, Politically Exposed Persons mean State or Government Heads entrusted with top level public office, and high level politicians, government officials, judicial or military personnel, political party officers and representatives at critical positions, and the persons that can be characterized as executives of public institutions in a foreign country. Before any person covered by this definition is accepted as customer, special know-your-customer principles are applied and prior consent of the top executive management of the Bank is received.
- (g) 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.
- (h) 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.
- (i) In money transfers made through the Bank within the limits set forth in the Regulation on Prevention of Laundering Proceeds of Crime and Financing of Terrorism, the Bank includes and verifies the following information on the sender:
  - I. Full name, the title of the legal entity registered with the trade registry, the full name of other legal entities and unincorporated entities,
  - II. Account number, and reference number related to the transaction in case the account number is not available,
  - III. 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 money transfer messages, information on the recipient as specified in clauses (I) and (II) of this paragraph shall also be included. Verification of such information is not obligatory. Any incoming money transfer that does not contain the information in clauses (I), (II) and (III) shall be returned or the missing information shall be completed via the financial institution that sent this message. 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.
- (j) The Bank in no event accepts the opening of any account unnamed/anonymous or in the name of any person other than its real known holder.
- (k) Correspondent Banking: The bank shall take following necessary measures in foreign correspondent relationships;
  - 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.
  - Approval of the top manager of the correspondent financial institution should be received, and the obligations of each organization should be documented before establishing correspondent relations;
  - Assess anti-money laundering and terrorist financing system of the respondent financial institution and to ascertain that the system is appropriate and effective
  - With regard to correspondent accounts, it should be guaranteed that the customer identity information are confirmed by the bank, that "attention" clause regarding the customers who have direct access to the accounts of the correspondent bank is fulfilled, and that identity information of the related customer can be submitted to the correspondent bank upon request. 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 work flows for which top executive's approval is required.

- (l) The Bank pays utmost attention against the risk of use of the opportunities created by new and developing technologies for the purposes of laundering of money and financing of terrorism, and takes appropriate measures for prevention purposes.
- (m) 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. In order to rely upon a third party as above, the Bank must make sure that the counterparty complies with requirements of the know- your-customer principle and rules, and that certified copies of identity documents will be submitted and furnished upon demand. The principle of trust in third parties shall not apply if the third party resides in risky countries.
- (n) 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.

## **ELEVENTH PART**

### **Updating**

**Article 23:** This Internal Regulation will, if and when deemed necessary, be updated by the authorized officers for submission to the Board of Directors for approval.

## **TWELFTH PART**

### **Effective Date**

**Article 24:** This Internal Regulation will become effective upon the Board of Directors approval.