BANK POLICY ON COMPLIANCE WITH OBLIGATIONS OF PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

1. INTRODUCTION

Albaraka Turk Participation Bank A.Ş., its branches and subsidiaries including abroad are committed to cooperating with all national and international efforts to fight against money laundering, terrorist financing, and other financial crimes, and to act in accordance with the relevant regulations.

1.1. Purpose

a) To ensure the Bank's compliance with obligations on anti-money laundering and prevention of terrorist financing,
b) To determine strategies for reducing the exposure to possible risks by evaluating customers, transactions and services with a risk based approach, and, to determine internal controls and preventive actions, operational rules and responsibilities,
c) To create awareness among Bank staff about these topics.

1.2. Definition of Terms

Bank	:	Albaraka Turk Participation Bank (Albaraka Türk Katılım Bankası A.Ş.)
ABG	:	Albaraka Group BSC (c)
CBB	:	Central Bank of Bahrain
Ministry	:	Ministry of Treasury and Finance
MASAK	:	Ministry of Finance Financial Crimes Investigation Board of Turkey
Proceeds of Crime	:	Means proceeds derived from crime
Laundering	:	Means taking proceeds of crime abroad or hiding their illegitimate source and using certain processes in order to form the opinion that they were acquired via legitimate ways,
Laundering offence	:	Means the offence defined in article 282 of Turkish Criminal Law No.5237 dated 26/09/2004.
Financing Terrorism	:	Means providing or assuring money or every asset that can be represented with money, rights, debt receivable and interest to be used wholly or partially to commit terrorist acts
AML/CFT	:	Anti-Money Laundering/Combating the Financing of Terrorism
FATF	:	Financial Action Task Force
Law No. 5549	:	Means the Law No. 5549 on Prevention of Laundering Proceeds of Crime dated 11/10/2006
Law No. 6415	:	Means Law No. 6415 on Prevention of the Financing of Terrorism dated 7/2/2013
Law No. 7262	:	Means Law No. 7262 on Prevention of the Financing of Proliferation of Weapons of Mass Destruction dated 27/12/2020
Permanent Business Relationship:		Means a business relationship that is established between obliged parties and their customers through services such as opening an account, lending loan, issuing credit cards, safe-deposit boxes, financing, factoring or financial leasing, life insurance and individual pension, and that is permanent due to its characteristics
Politically Exposed Person	:	Senior individuals who are entrusted with significant public duties through election or appointment domestically or in a foreign country, as well as board members, senior executives, and others holding equivalent positions in international organizations

Compliance Officer	:	Means the officer assigned by obliged parties who is vested the required authority for ensuring compliance with obligations introduced by law and legislation effected based on the law.
Customer Risk	:	Means 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,
Country Risk	:	Means the risk which is possible to be exposed by the Bank due to business relationships and transactions with citizens, companies and financial institutions of the countries that are announced by the Ministry or Legislation and Compliance Department 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,
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
Freezing of Assets	:	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

1.3. Scope

This Policy is created by considering the size of the business, the volume of business and the nature of the transactions carried out, as well as the issues specified within the scope of the national risk assessment. The document is valid for the Headquarters and all branches of the bank including those abroad.

1.4. General Framework

Legislation and Compliance Department must take necessary actions to ensure that the entire staff members of the Bank have standard level of knowledge and information regarding the following subjects, and update the information when required:

a) Concepts of crime proceeds and laundering crime proceeds.
b) Stages of money laundering.
c) Methods of money laundering.
d) Historical development of the combat against money laundering, international actors and multilateral agreements.
e) Prevention of funding terrorism;
   - The main sources of funding terrorism. (Legal or illegal activities)
   - Similarities and differences between money laundering and funding terrorism.
f) Prevention of corruption, and combat against bribery and similar financial crimes;
   - Concept of corruption and the importance of the struggle against it.
   - Ethical principles of the Bank.

While preparing this Policy, recommendations, principles, standards and guides created by generally accepted institutions (FATF, Basel Principles, etc.) and ABG policies and procedures, which were established by ABG in accordance with CBB legislation, are considered as far as they do not contradict the Laws numbered as 5549, 6415 and 7262 and the relevant legislation. This Policy is prepared in accordance with the Law and the regulations and communiqués issued pursuant to the Law, with the participation of all relevant departments within the Bank as far as possible and under the supervision and coordination of the Compliance Officer. However, if necessary, the opinions of the regulatory authorities, the Bank's Senior Management, the relevant committees in the Bank or the ABG Compliance Team can be obtained depending on the content

and importance of the subject; and if necessary, external service can be obtained from experts who are qualified and appropriate.
If there is a difference between this Policy and local legislation in the countries where the bank operates, the stricter provisions are followed.
Issues such as who is responsible for all measures and operating rules specified within the scope of the policy, who or which departments will be responsible for the approval, realization, reporting and monitoring of transactions according to certain risk limits are subject to procedure. In determining the procedures, duties and authorizations are made in such a way that the staff who will take part in the monitoring, control and supervision of the Bank's transactions and work-flows according to risks are not also the staff already performing these operations.

1.5. Legal Regulations and Responsibilities
The Bank's staff are responsible to know all legal and administrative obligations especially the Laws numbered as 5549, 6415 and 7262 in the fight against money laundering and the financing of terrorism, and the regulatory and supervisory institutions involved in the fight against money laundering and the financing of terrorism.

1.6. Duties, Responsibilities and Powers of the Legislation and Compliance Department
Duties, responsibilities, and authorities of the Legislation and Compliance Department are determined by the Legislation and Compliance Department Charter, which is approved by the Board of Directors of the Bank. The Department directly works in affiliation with the Audit Committee and the Board of Directors.

1.7. Duties, Responsibilities and Powers of the Compliance Officer
Duties, responsibilities and authorities of the Compliance Officer who is appointed by our Board of Directors, are stated here below;

1. Sustaining risk management, monitoring and control activities by taking into consideration the risks determined within the scope of training, research, development, surveillance, national risk assessment in order to ensure the compliance of the Bank with the Laws numbered as 5549, 6415 and 7262, and also regulations and communiqués issued pursuant to the Laws, and to provide the necessary communication and coordination with MASAK,
2. Ensuring that the compliance control activities are executed at the Bank within the framework of the regulation published by BDDK.
3. Establishing and developing Bank policies and procedures regarding AML/CFT and presenting the Bank policies to the approval of the Audit Committee and the Board of Directors.
4. Regarding AML/CFT;
   a) Creating the risk management policy, conducting risk management activities,
   b) Creating monitoring and control policies, and conducting relevant activities,
   c) Preparing the training schedule, presenting the aforementioned to the approval of the Board of Directors and ensuring that the training schedule is efficiently implemented.
   d) Taking the necessary precautions in order for the defaults detected by the Internal Audit and Internal Control Departments or the relevant and competent authorities to be corrected.
5. Presenting reports regarding Department activities to the Audit Committee and the Board of Directors at regular intervals.
6. Investigating and evaluating, with his power and facility, the information and findings regarding suspicious transactions that he may have learned on his own initiative or conveyed to him, and reporting the transactions he deems suspicious to MASAK.
7. Taking the necessary precautions for ensuring the confidentiality of notifications and other issues.
8. Regularly keeping the information and statistics about the internal auditing and training activities and sending them to the MASAK within the legal duration stated in the regulation.
9. Demanding all information and documents from all of the departments within the bank in connection with their own field of duty.
10. Preparing Department budget annually and presenting it to the Audit Committee to get the Board of Directors' approval.

11. Presenting Department budget accruals to the Audit Committee periodically.
12. Establishing the human resources number that the Department shall need annually, presenting it to the approval of the Audit Committee and transmitting it to the relevant unit of business following the approval on the purpose of implementing of the recruiting processes.
13. Taking the approval of the Audit Committee for the appointment of the staff of the Department to another department or branch within the bank.
14. Making the decision that the staff of the Department is temporarily assigned at another department or branch within the bank.
15. Making recommendations to the Audit Committee regarding the salaries, compensations, travel allowances and all other payments to be made to the Department staff.
16. Explicitly establishing the duties, authorities and responsibilities of services within the Department and approving the working principles and procedures of the staff assigned at these services and ensuring the appropriation of the necessary resources.
17. To perform duties and authorizations to ensure that the staff who shall be responsible for monitoring, controlling and supervising the transactions and workflows carried out at the Bank according to risks are not also the staff performing these transactions.
18. Ensuring the attendance of the Department staff to training programs in order to ensure their occupational adequacies and developments.
19. Making offers to the Audit Committee to be presented for the approval of the Board of Directors to make changes to the relevant policies and the Department Charter in regard to the legislation changes that occur in time.
20. Conducting coordination and cooperation with ABG in issues that fall under the field of duty and conducting the necessary correspondences.
21. Expressing opinions or ensuring that opinions are expressed for the activities planned to be implemented with new products and transactions before taking approval from the Board of Directors as per the "Regulation on Internal Systems and Internal Capital Adequacy Assessment Process of Banks".
22. Ensuring that the Bank staff is notified as soon as possible regarding the changes in the policies and rules within the bank with the legislation.
23. Ensuring that the mechanisms that will allow obligations brought on by the legislation are fulfilled within the framework of the compliance controls are established and reporting them to those concerned.
24. Monitoring local and international developments and regulations in issues that are relevant to his field of duty; and attending the trainings, webinars, meetings, seminars or conferences taking place locally or abroad, if the Audit Committee Chairman deems necessary.
25. Making correspondences, attending meetings and expressing opinions on behalf of the Department.
26. Assigning duties and responsibilities to the Consultant if any, as he deems necessary.
27. Establishing the information sharing policy of the financial group and taking the necessary measures regarding the safe sharing of this information within the group.

The compliance officer may delegate, expressly and in writing, some or all of his duties and powers to the assistant compliance officer. The transfer of the said duty and authority does not remove the responsibility of the compliance officer in this regard. Assistant compliance officer is appointed exclusively as a staff of the Bank, reporting to the compliance officer. Assistant compliance officer is appointed for the same term and in line with same procedure as the compliance officer.

2. RISK MANAGEMENT POLICY

2.1. Purpose:

Identifying, rating, monitoring, evaluating and reducing potential risks on the Bank by considering customer risk, service risk and country risk. . The Risk Appetite of the Bank on AML/CFT is generally prudent.
It is ensured that the risk identification and evaluation methods, risk rating and classification methods are questioned retrospectively through case studies or finished transactions, are re-evaluated and updated according to the conclusions reached and to developing conditions.

2.2. Knowing the Customer

The most effective way to protect the Bank from money launderers is to establish, and strict adherence to, policies, principles and rules in compliance with the related legislation based on "know your customer" principle. The aim is to achieve full clarity about the customers' information and banking operations while creating and maintaining a relationship based on mutual trust.

2.2.1. Admission of Customer - Common Principles

During the admission of customer, in order to prevent the Bank from being exploited for money laundering, the Legislation and Compliance Department must have sufficient information about customers regarding the followings:

a) In relation with its identity, to check and verify the information and documents listed/sought in the legislation,
b) Consistency of documents and information provided by customer,
c) The purpose of customer in preferring the Bank and opening the account,
d) Profession of the customer, the main line of business that generates its income,
e) The capacity and profile of its transaction with the Bank,
f) The business venue, office or workshop of the customer,
g) The reputation of customer in the market,

and, in order to create a sound and trustable relationship between the Bank and the customer the Legislation and Compliance Department must make necessary in-house arrangements and issue circulars within the Bank.

In this context, the demands of the persons to enter into a permanent or temporary customer relationship are evaluated within the scope of related policies and procedures, primarily the Sanctions Policy approved by the Bank's Board of Directors, taking into account the types of services to be provided.

Furthermore, utmost attention shall be paid to the following points:

a) The Bank must be protected against international crimes by transactions of money laundering based on adaptation and application of the principles in this policy by all staff of the Bank.
b) Giving maximum attention and care to the acceptance of persons and institutions as customers of the Bank whose wealth and funds are subject to suspicion of legitimacy.
c) In line with the general principle that bank's relationship with its customers should be based on mutual trust, clarity and exchange of information, those persons who abstain from filling in the necessary documents and identification forms or who present misleading or non-confirmable information shall not be accepted as customers.
d) It will be made sure that no accounts are opened under symbolic or anonymous names or on behalf of third parties.
e) A continuous surveillance shall be done to observe whether or not the person literally uses the account which is opened on behalf of him/her.
f) Maximum care and attention should be paid in the requests of third parties to open an account on behalf of one or more persons by power of attorney (Except, the accounts for persons or children who are under tutelage or guardianship). It is necessary to pay attention to the fact that the power of attorney / instructions are in the format determined by the relevant units of the Bank and have been approved by the notary public in the transactions performed with the power of attorney and the approval of the institutions that issue the document should be taken if the customer is not well known.
g) The age limit of accounts which belong to children shall be controlled.
h) Private and retail banking or credit relationship will not be instituted with possible clients if prior assessment yields a suspicion on the documents or information about the assets of the persons and banks indicating that these assets were earned illegally. The guarantee and collaterals of these people will not be accepted even if they are not direct clients.
i) Risky banking services such as;
    a. Renting safe deposit boxes,
    b. Admitting personal checks in fx for collection, or giving letters of guarantee against cash blockage, shall not be provided,

    to those customers who are not very well known and respectable.

2.2.2. Customer Admission and Responsibilities

During the process of filing new customers for the Bank, the identity of customer shall have to be determined. His/her address shall be recorded; and legally necessary documents and data shall be sought and taken. Ratification of these data shall be done and kept in physically and/or electronically safe boxes or files.
For this purpose, crosschecks are made through Central Population Management System (MERNİS) system, the Turkish Republic's ID number, Ministry of Treasury and Finance Tax ID Number and Foreign ID Number. After the control, if the information don't match or other unfavorable situations occur (eg. death record etc.), related Head Office departments only shall make decision about admission of the customer.

2.3. Principles on Identity Check

Identity verification is carried out in accordance with procedures, workflow charts, manuals, instructions, etc., formed based on the type of customer.
. All this documentation is kept on the intranet accessible to Bank staff.
Additionally, in terms of the method of identity check,

a) The Bank shall identify customers or those who act on behalf or for the benefit of customers by receiving their identification information and verifying it;
   - When establishing permanent business relationships, regardless of the monetary amount,
   - When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than the amount specified in the Regulation on Measures to Prevent Money Laundering and Financing of Terrorism,
   - When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than the amount specified in the Regulation on Measures to Prevent Money Laundering and Financing of Terrorismin wire transfers;
   - In cases requiring suspicious transaction report, regardless of the monetary amount,
   - In cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information, regardless of the monetary amount
b) Customer identification shall be completed before the business relationship is established or the transaction is conducted. Before establishing a business relationship, sanction list controls shall be completed
c) When establishing permanent business relationship, information on the purpose and intended nature of the business relationship shall be received
d) In the context of control of the authenticity of documents subject to verification, if the truths of documents which are used to verify the customer identity are suspicious, the genuineness of documents must be confirmed by approaching to the person, institution or other public agent issued these documents as long as it is possible.
e) Systematic verification of the information and data about legal existence and structure of the customer (legal person), real name or title, address, directors and licenses of company, documents legally binding the company and defining authorities in the company, must be made by comparison with the official public records of the State (MERNİS, TCKN,VKN, etc.).
f) In the context of customer identification in subsequent transactions, in the subsequent face-to-face transactions which require identity check and that are conducted in the scope of permanent business relationship of those who were duly identified formerly, identity data shall be received and compared with the data already available to the Bank. 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 through comparing the data stated on these documents with the data already available to the Bank. As to the subsequent transactions requiring identity check 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.
g) According to the risk scores assigned within the scope of the criteria determined by the Legislation and Compliance Department, the documents and information regarding the identification of the existing customers are updated;
   • Annually for high-risk customers,

• Once in every two years for medium risk customers,
• Once in every three years for low risk customers

Identification processes according to customer types and other issues in this process are listed below.

2.3.1 Customer Identification of Natural Persons

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 of job and profession, telephone number and fax number if any, e-mail; and as additional information for Turkish citizens, T.R. identity number and for foreigners place of birth shall be received.
2) Name and surname, date of birth, mother's and father's name, nationality, type and number of the identity card of the person concerned shall be verified through
   a) T.R. identity card, T.R. driving license or passport for Turkish citizens;
   b) Passport, certificate of residence or any type of identity card considered proper by the Ministry for non-Turkish citizens. 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.

In the establishment of permanent business relations with individuals, remote identification methods can be used to verify the identity of the customer by taking the methods to be applied in remote identification and other measures within the scope of customer identification, provided that they comply with the provisions of the relevant legislation on this subject.

2.3.1.1 General Principles for Remote Identity Verification for Natural Persons

1. In the remote identity verification of natural persons or sole proprietors, the information mentioned in the Article 2.3.1. and the written declaration mentioned in Article 2.3.9 are obtained using the methods and procedures applied in remote identity verification. Information required as part of enhanced measures for identity verification and remote identity verification can also be submitted through forms filled out electronically via channels such as websites, internet banking, or mobile applications. For verification purposes, the ID card defined under the Turkish Republic Identity Card Regulation is used. The address and identity information obtained within the scope of identity verification are also confirmed by querying the database of the Identity Sharing System of the Ministry of Interior's General Directorate of Population and Citizenship Affairs.
2. During the remote identity verification process, measures are taken to verify the authenticity of the individual's identity and the identity document. In this context, methods to determine the validity of the identity document and the individual's liveliness are used, ensuring that the photograph and personal information on the identity document match the individual.
3. At a minimum, the following measures are taken under the second paragraph:

   a) The identity document is verified using near-field communication. If this is not possible, at least four security features on the identity document are verified in terms of shape and content.

   b) A biometric comparison is conducted between the individual's face and the photograph from the contactless chip on the identity document, if accessible via near-field communication, or the photograph on the identity document. Additional measures are taken to prevent risks related to fake face technologies.

c) A one-time password specific to the identity verification process is sent to the individual via electronic communication service providers. If the transmitted password is approved in the system, the individual's mobile phone number is verified.

2.3.2 Customer Identification of Legal Persons Registered To Trade Registry, Non-Resident Legal Persons and Trust Agreements Established Abroad

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 and for foreigners place of birth 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 2.3.1; 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 submitted to them 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.
7) Customer identification of non-resident legal persons shall be made through copies of the documents approved by the consulates of the Republic of Turkey corresponding to the documents in related country required for legal persons residing in Turkey or through the copies of the documents attached apostille by an authority of the country which is a party to the “Convention on Abolishing the Requirement of Legislation for Foreign Public Documents”. Also, in the framework of risk-based approach, when necessary, identity information shall be verified through notarized Turkish translations of copies of the documents.
8) In case a transaction request, which requires identification check, on an account of a Trust established abroad by an individual or legal person trustee determined in the contract, it must be declared in writing that the transaction is requested on behalf of the assets created under the trust agreement, in accordance with Article 15 of the Law, before these transactions are realized. Identification under a trust agreement established abroad; it is made on the written copies of the trust agreement approved by the consulates of the Republic of Turkey or through the copies of the documents attached apostille by an authority of the country, which is a party to the “Convention on Abolishing the Approval Requirement Legislation for Foreign Public Documents”. In the framework of risk-based approach, identity information shall be verified, when necessary, through notarized Turkish translations of copies of the documents. Identification information of persons authorized to represent the trustee shall be verified through the documents mentioned in article 2.3.1 and this article. Within the scope of determining the real beneficiary, the identity information of the contract founder, beneficiary or beneficiary groups and, if any, persons designated as the auditor under the contract is taken and reasonable measures are taken to confirm the information. Necessary measures are also taken to reveal the real person or persons who ultimately control the said assets.
   A trust agreement is aimed to mean; a legal relationship that provides for the transfer of an asset to a certain beneficiary or group of beneficiaries by the founder of the contract, who is the owner of the asset, to a trustee executing the contract for the purpose of management, use or other dispositions specified in the contract.

2.3.2.1 General Principles for Remote Identity Verification for Legal Entities Registered in the Trade Registry

1) For remote identity verification of legal entities registered in the trade registry, the information related to the legal entity mentioned in the first paragraph above and the written declaration regulated in Article 2.3.9 are obtained using methods and procedures applied in remote identity verification. Information required under the first paragraph of Article 2.3.1 for identity verification can also be submitted through forms filled out electronically via channels such as websites, internet banking, or mobile applications.
2) Among the information related to the legal entity, the title, trade registry number, field of activity, and address are verified through the Central Registry Record System (MERSİS) defined in Article 4 of the Trade Registry Regulation, and the Turkish Trade Registry Gazette, while the tax identification number is verified through the current information in the database of the Revenue Administration.
3) Remote identity verification of the person authorized to represent the legal entity is carried out by obtaining the information required for authorized representatives, as stated in the first paragraph above. If there are multiple individuals authorized to jointly represent the legal entity, their identity verification can be conducted in the same session or at different times.
4) If the person authorized to represent the legal entity is already a customer of the Bank, they can request to establish a permanent business relationship for the legal entity they represent through the internet banking or mobile application they have access to. In this case, the process of identity verification for the legal entity continues seamlessly after the individual logs into the mentioned applications and their identity is verified.
5) The individual's authorization to represent is confirmed by matching the information obtained with the current data retrieved from MERSİS or the Turkish Trade Registry Gazette. In this context, if necessary, photographs and/or screenshots showing the details of the signature circular provided by the authorized representative are created, the signature sample obtained from the signature circular is compared with the individual's identity document and/or signature sample found in MERSİS, and the existence of the signature circular is verified using the date and journal number recorded on it.
6) Necessary measures are taken to identify the ultimate beneficial owner. In this context, documents and procedures defined for remote identity verification of natural or legal persons can be utilized.

2.3.3 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, 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 and for foreigners place of birth 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 identification number documents issued by the relevant unit of the Revenue Administration, the identification information of the person authorized to represent the association shall be verified through identity cards stipulated in Article 2.3.1; 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, 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 T.R. identity number and for foreigners place of birth 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 identification number documents issued by the relevant unit of the Revenue Administration; the identity information of the person authorized to represent the foundation shall be verified through identity cards stipulated in Article 2.3.1; 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.

2.3.4 Customer Identification of Trade Unions and Confederations

1) In customer identification of trade unions and confederations the name of the organization, its aim, registry 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 of the person and sample signature of the person authorized to represent the trade unions and confederations and for Turkish citizens the additional information as T.R. identity number and for foreigners place of birth shall be received. The information gathered shall be verified through charter of these organizations and the records kept by local directorates of Ministry of Family Labor and Social Security, tax identification number documents issued by the relevant unit of the Revenue Administration; the identity information of the person authorized to represent the organization shall be verified through identity cards stipulated in Article 2.3.1; and the authority to represent shall be verified through documents of registration or documents of authorization to represent.
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.

2.3.5 Customer Identification of Political Parties

1) In the customer identification of political parties, the name of the relevant unit of the political party, 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 card and sample signature of the person authorized to represent and for Turkish citizens the additional information as T.R. identity number and for foreigners place of birth shall be received. Name and address of the relevant unit of the political party shall be verified through their charter identity of the person authorized to represent shall be verified through the identity documents stipulated in Article 2.3.1, the authority to represent shall be verified through documents of authorization to represent.
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.

2.3.6 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, 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 and for foreigners place of birth shall be received. The identity information of the person authorized to represent the organization shall be verified through the identity documents stipulated in Article 2.3.1, and the organization information and the authorization of the person acting on behalf of the organization shall be verified through 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, 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 and for foreigners place of birth 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 through identity documents stipulated in Article 2.3.1, 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.

2.3.7 Customer Identification of Public Institutions

In transactions in which the public administrations in the scope of general administration in accordance with the Public Financial Management and Control Law No. 5018 and quasi-public professional organizations are customers, the person making transactions on behalf of these bodies shall be identified in accordance with Article 2.3.1. Authorization is verified through the certificate of authority arranged in accordance with the legislation.

2.3.8 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;
   a) Customer identification of legal persons and unincorporated organizations shall be carried out in accordance with Articles 2.3.2 and 2.3.6.
   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 2.3.1. In cases where the customer identification of the person authorized to represent cannot be carried out through the identity documents specified in Article 2.3.1, 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 2.3.1. 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 2.3.1, 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 2.3.1.
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.

2.3.9 Customer Identification of Those Acting for the Benefit of Others

1) The Bank is required to take necessary measures in order to detect whether action is carried out for the benefit of another person. Within this scope, the Bank puts up required notices in workplaces where they run service in a way that all customers can easily see in order to remind the persons, who act in their own name but for the benefit of others, of their responsibilities. In addition, the Bank receives, 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. This declaration can be specified in the customer contract or be received by using appropriate forms.

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 requesting the transaction and the identity of the person for the benefit of whom the transaction is conducted is identified.
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 is applied.

2.3.10 Identification of Beneficial Owner

1) The Bank takes necessary measures in order to detect the beneficial owner.
2) When establishing permanent business relationship with legal persons registered to trade registry, the Bank identifies, in accordance with article 2.3.1, the natural person partners holding more than twenty-five percent of the legal person's shares as the beneficial owner.
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. And natural person(s) detected shall be considered as beneficial owner.
4) In cases where the beneficial owner is not detected within the scope of paragraphs 2 and 3, the natural person(s) holding the position of senior managing official, whose authorization to represent the legal person is/are registered to trade registry, shall be considered as beneficial owner.
5) Within the scope of 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 is not detected, the natural person(s) holding the position of senior managing official within them shall be considered as beneficial owner.
6) In the scope of the paragraphs (1) to (5), the Bank identifies the beneficial owner and take necessary measures in order to verify the beneficial owner. In this framework, a notarized circular of signature including identity information can be used.
7) When establishing permanent business relationship with legal persons registered to trade registry, the Bank identifies, in accordance with article 2.3.2, the legal person partners holding more than twenty-five percent of the legal person shares. The confirmation of the identity information required to be obtained within this scope of the legal entity partners residing abroad can be made through the open sources of the equivalent institutions of the Union of Chambers and Commodity Exchanges of Turkey in the relevant country or other institutions where the relevant data is kept officially.

2.3.11 Reliance on Third Party

1) The Bank can establish business relationships or carry out transactions by relying on measures taken related to the customer by another financial institution on identification of the customer, the person acting on behalf of customer and the beneficial owner, and on obtaining of information on the purpose of business relationship or transaction. In such a circumstance, the ultimate responsibility shall remain with the financial institution carrying out transaction by relying on the third party under the Law and the related regulations.
2) Reliance on third parties shall be 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 terrorist financing in accordance with international standards if the third parties are resident abroad,
   b) The certified copies of documents relating to customer identification shall immediately be provided from the third party when requested.
3) The financial institution, which establishes a business relationship or conducts a transaction by relying on a third party shall immediately receive the identity data of the customer from the third party.

4) The transactions which the financial institutions conduct between themselves on behalf of customers and relationships between financial institution and its agents, similar units or outsourcing entities are not within the scope of the principle of “reliance on third parties.
5) The principle of “reliance on third parties” may not be applied to the cases where the third party is resident in a risky country.

2.3.12 Enhanced Measures to Be Taken in Remote Identity Verification

1. A risk assessment is conducted to create and evaluate the customer profile upon the customer's application. In this context, in addition to the information required under the obligation of identity verification, the following minimum information is obtained: the purpose and nature of the business relationship (account opening purpose, requested products, etc.), the source of the assets and funds subject to the transaction, average income information, and the estimated monthly transaction volume and number for the account to be opened.
2. If subsequent transactions within the scope of a continuous business relationship established via remote identity verification are conducted face-to-face with the obligated party, identity verification is performed in accordance with the procedures in Articles 2.3.1 and 2.3.2, and a signature specimen is obtained.
3. In remote identity verification processes, one or more of the measures listed below, or all of them, are applied proportionally to the risk identified within the framework of a risk-based approach:

   a) Obtaining additional information about the customer and updating the identity information of the customer and the ultimate beneficiary more frequently.

   b) Requiring the approval of a higher-level officer for entering into the business relationship, maintaining the existing business relationship, or performing the transaction.

   c) Keeping the business relationship under strict supervision by increasing the number and frequency of controls and determining transaction types that require additional control.

   d) Requiring the first financial transaction in the establishment of a continuous business relationship to be conducted through another financial institution where customer identification principles are applied.

   e) Monitoring transactions that are not appropriate to the customer's financial profile and activities or unrelated to their activities.

   f) Taking appropriate and effective measures, including setting limits on the amount and number of transactions.

4. In cases where the identity document cannot be verified using near-field communication during the remote identity verification process, as an additional method, it is mandatory for the first financial transaction to be conducted through an account at another financial institution where the customer identification principles are applied, prior to the establishment of the continuous business relationship.

2.3.13 Rejection of Transaction and Termination of Business Relationship

1) Where the Bank cannot make customer identification or obtain information on the purpose of the business relationship, cannot establish business relationship and not conduct the transaction, which the Bank is requested. In such a circumstance, the Bank cannot open an anonymous account or account in a fictitious name.

2) In cases where customer identification and its verification which are required to be conducted due to suspicion on the adequacy and accuracy of the previously obtained customer identification information cannot be carried out, the business relationship shall be terminated.
3) The Bank assesses whether the situations specified in the first and second paragraphs of this Article are suspicious transactions or not.

2.4. Persons Ineligible as Customer

2.4.1. Persons of Unidentified Address and Identity

Persons and institutions who desire to open an account with the Bank under a different name, abstain from filling up the Customer Bio-data Forms or unwilling to provide other explanatory details required for customer identification, or giving misleading and un-verifiable information shall not be accepted as customers.

2.4.2. Persons and Organizations Blacklisted by Public Authorities in Context of Combat Against Funding Terrorism and Money Laundering

Persons and organizations whose names appear in the lists (List of relevant institutions in the Sanctions Policy of the Bank, primarily the UN and OFAC) issued or to be issued by international and/or local public offices and/or legal institutions engaged in combat against crime revenues shall not be accepted as customer. If in later stages any such negativity emerges about persons or organizations (i.e. banks, companies, etc.) among the customers, the relationship with them shall be ended and their transactions shall not be mediated again. Such cases shall be reported to MASAK as suspicious transactions.

2.4.3. Mail-Box Banks

The banks (shell banks) without any physical address, full time employee/s, unbounded to any public authority in terms of banking operations, licensing, registration and auditing, unattached to any reputable banking organization that has regulations and auditing procedures acceptable by banking practices with regard to prevention of laundering the revenues derived from crime proceeds shall not be accepted as customer and their transactions must not be mediated by the Bank, directly or indirectly.

2.5. Regions, Persons and Transactions Requiring Special Attention for their Admission as Customer

Persons and institutions operating in the sectors and geographical areas stated below, are considered as carrying higher risk for exploiting the Bank with the purpose of money laundering.

2.5.1. Risky Regions

Transactions from domestic and foreign regions, which will be determined by the Legislation and Compliance Department, shall be considered as carrying high risk. Identity checks and verification procedures for customers living or connected to the risky regions shall be applied with utmost care and in a more controlled manner while executing their transactions.

2.5.1.1. Non-Cooperative Countries

Working relationship with citizens, firms and financial institutions of the countries blacklisted by FATF (in the List of Non-Cooperative Countries) for not complying with its recommendations, or, implementing them in part shall not be established. However, if any transaction is made, utmost attention must be given to it. If the visible economic and legal aim of the transaction is not reasonable or logical, necessary investigations shall be conducted, the findings must be recorded and kept in the transaction file.

2.5.1.2. Grey Areas

The procedures of “knowing the customer” shall be applied more carefully in case the customer (or related transaction) is settled in un-democratic countries and territories where the rate of crimes resulting from smuggling and terrorism is high, corruption and bribery is widespread, and which are on illegal drugs manufacturing and distribution routes. Any suspicious situation shall be reported as required legally.

2.5.1.3. Offshore Centers, Free Zones and Financial Hubs

The procedures of “knowing the customer” shall be implemented meticulously in case the customer is settled in or the transaction is connected to offshore centers, free zones or international finance centers where rigid

secrecy rules are applied on banking transactions. Such international money orders, in which the ordering party (the name and/or the title of the orderer) is not clearly mentioned, shall not be processed. The transaction shall be reversed to the originator by related operations department of the Bank.

2.5.2. Risky Customers

2.5.2.1. Politically Exposed Persons (PEP's)

Since, the Politically Exposed Persons in countries where corruption is particularly widespread may exploit their political influence for self-enrichment through receiving bribes, embezzlement and in similar ways, they are considered among risky customer type.

The process of opening account for Politically Exposed Persons is subject to the approval of the related branch/regional manager and Head of Legislation and Compliance Department. The requirements of know your customer principle are more intensely applied to those with Politically Exposed Persons.

2.5.2.2. Persons Known as Involving in Criminal Activities or Dealing with the Activities Considered Suspicious by General Public

2.5.2.3. The Customers who are Located, Operating or Transacting in Countries where Necessary Legal Regulations on Combat Against Criminal Revenues are not in Place

In this context, necessary information is provided throughout the bank by the Legislation and Compliance Department.

2.5.2.4. Relationships with Risky Countries

The Bank is required to pay special attention to business relationships and transactions with the natural and legal persons, unincorporated organizations and the citizens located in risky countries and to obtain information about the purpose and the nature of the transactions, as far as possible, which have no apparent reasonable legitimate and economic purpose and to record them.

Regarding these countries, necessary information and awareness across the bank are provided through training, announcements, and system warning mechanisms implemented by the Legislation and Compliance Department.

2.5.2.5. Waqfs (Charity Organizations) and Associations

While branches open account/s for the above stated establishments, open identity of the persons or institutions, main line of their activity, purpose of opening the accounts, expected accounts transactions and services, method of opening the accounts, destinations of incoming and outgoing funds (Cash, EFT, Swift, Local and International) and details about their founders, their authorized representatives, and senior managements must be collected. In addition, the Enhanced Due Diligence forms prepared by the Legislation and Compliance Department for the better knowing the customers within this scope should be filled in detail by the branch and added to the customer documents. Branch managements must take necessary precautions to ensure the recording of all information gathered. This information must be checked during branch inspections.

2.5.2.6. Correspondent Banking

The following points must be taken into consideration while establishing a correspondent banking relationship. About the bank with which the relationship will be established;

a) The nature and subject of activity, reputation and adequacy of its internal and external audits shall be determined through publicly available data about the bank,
b) Whether the bank has gone under any investigation, inquisition, prosecution, penalized or warned on charges of money laundering and funding terrorism must be surveyed,
c) The methods that it uses to prevent money laundering and funding terrorism shall be checked and its level of appropriateness to the necessity of "know your customer" must be assessed.
d) Approval of Assistant General Manager of the Bank to whom International Banking Department reports shall be received before starting a new correspondent banking relationship.
e) It must be assessed whether the correspondent bank has any customer directly accessing its accounts, and if so, whether the obligation of special attention to these customers is fulfilled.

In order to prevent faults in the communication and lack of any information in the records questionnaires with the above mentioned data are collected. The questionnaire must be preserved in the correspondent-banking file in order to be given to auditors when requested.
The Bank does not establish any correspondent relationship, if the answers provided in the questionnaire filled by the interested bank are found inadequate in terms of prevention of crime revenues precedents.

2.5.2.7. Sensitive Sectors and Professions
Utmost attention must be paid while opening accounts for persons or organizations from sectors and occupation groups which will be determined by Legislation and Compliance Department. Customer identification documents, sector information shall be recorded carefully and completely. The customers'' accounts shall be kept under constant and attentive scrutiny. Account activities of those customers must be controlled in branch audits.

2.5.3. Risky Transactions
Risky transactions are customer funds and transactions resulting from ambiguous activities and the activities unrelated with main business line of the orderer. They are generally cash transactions, electronic transfers and the financial products issued in the form 'to the bearer' (cheques etc.) products.

2.5.3.1. Cash Operations
The controls and documentation of transactions that can normally be processed through the bank accounts are desired to be affected in cash by customers, shall be done with utmost care. Branch operator must pay more attention during approval stage of accounting receipts and payment slips of such transaction.

2.5.3.2. Electronic Fund Transfers
1. In domestic and international electronic transfer messages of the amount specified in the Regulation on Measures to Prevent Money Laundering and Financing of Terrorism or more, the sender's;
   a) Name and surname, title of the legal person registered in the trade registry, full name of other legal persons and entities without legal personality
   b) Account number, if the account number is not available, the reference number related to the transaction,
   c) At least one of the information that helps to identify the sender, such as address or date of birth or customer number, citizenship number, passport number, tax identification number,
   It is mandatory to include a place and the accuracy of this information is also confirmed.
   Electronic transfer messages also contain the information specified in subparagraphs (a) and (b) regarding the recipient, confirmation of this information is not obligatory.
2. In domestic and international electronic transfer messages below the amount specified in the Regulation on Measures to Prevent Money Laundering and Financing of Terrorism, the information specified in subparagraphs (a) and (b) above regarding the sender and receiver shall be included. Confirmation of this information is not obligatory.
3. In the chain of messages from the financial institution where the transfer order is given to the financial institution that will make the payment, the information required to be included in the electronic transfer messages regarding the sender is included by all financial institutions that mediate the transfer, and special attention is paid to the transfer of this information at every stage of the transfer.

2.5.3.3. Cashing of Personal Checks Drawn on Banks Abroad
Foreign exchange cheques drawn on organizations and/or persons abroad that do not have any bank account with the Bank or are not known by branches shall not accepted by the Bank for collection. The service of cashing foreign exchange cheques can be rendered only to persons or firms having solid commercial past and credibility, whose physical assets and business volume are in correlation with amounts of the cheques, and whose business ethics and commercial practices are known in detail.

2.5.3.4. Taking Measures against Technological Risks
a) Special attention shall be paid to the risk that the use of new and developing technologies, existing and new products, including new distribution channels, and opportunities brought by new business practices may be

used for money laundering and terrorist financing, and appropriate measures shall be taken for its prevention.

b) Appropriate and effective measures shall be taken including paying special attention to operations such as permanent business relationship, depositing, withdrawing and wire transfers which are carried out by using methods or systems enabling the institutions to conduct non face-to-face transactions, closely monitoring the transactions that are not consistent with financial profile or activities of the customer or do not have connection with his/her activities, and establishing a limit to amounts and number of transactions.

2.5.3.5. Credits Guaranteed By Cash Deposit

Credit applications made against the balances of bank accounts in free zones shall be rejected. Also the Guarantee Letters from the banks in these regions shall not be accepted as collateral.

2.5.3.6. Safe Deposit Boxes

a) Customers owning frequently used safe deposit boxes must be monitored specially by branches.
b) Customers shall not be left alone in safe deposit boxes' area.

2.5.3.7. POS (Point of Sale)

In payment services conducted via POS terminals, appropriate enhanced measures are applied for transactions requiring the establishment of a business relationship with the Bank and identity verification:

The regular checks ensure that these terminals are used appropriately for the intended purpose of the business relationship or under conditions permitted by the relevant legislation and are not used by other persons. In cases where non-compliance is detected, necessary measures, including the termination of the business relationship, are taken.

2.6. Suspicious Transactions

2.6.1. Description of Suspicious Transactions

The cases where there is a fact, a doubt or any reason leading to suspicion indicating that the money or any assets representing the value subject to transactions done by or done in the name of obligors is earned through illegal ways and means or there has been an attempt in doing so are considered Suspicious Transactions. The responsibility of reporting suspicious transactions belongs to all branches, representatives and similar units of the Bank in Turkey and abroad. If there is no information or a reason proving that the money or assets representing the money subject to the transaction in question is owned through legal means by the obligor, or, any reasonable doubt indicating that the income is connected to a crime of any sort, the transaction shall be considered as suspicious and it must be treated as such. Suspicious transaction reporting processes are established in abroad branches, representative offices and similar affiliated units in line with the legislation of the relevant countries.

2.6.2. Types of Suspicious Transaction

On reporting process, the "Suspicious Transaction Types" in the form of a guideline determined by the Financial Crimes Investigation Board, and international best practices are taken into consideration.

2.6.3. Detecting and Reporting Suspicious Transactions

Employees of the Bank should pay extreme attention while working with customers;

1. Who demand transactions that visibly have no legal or economic aim,
2. Whose income is not in correlation with and related to his/her business,
3. Who are unwilling to or abstaining from providing information and documents required in the context of legal obligations,
4. Who abstain from proceedings required for reporting and record keeping,
5. Who give misleading information or unverifiable data,
6. Who demand credits with no economic logic or without stating the purpose for the credits,

7. Who make transfers of money in large scales and in extraordinary amounts to geographically risky countries and territories,
   In case of encountering and suspicion of such transactions, the information and documents related to the transaction are attached and a notification is made to the Compliance Officer by using the channels determined by the Legislation and Compliance Department.
   In the process of reporting suspicious transactions, without considering whether the subject or the transaction is reported to MASAK by the Compliance Officer, one of the following decisions shall be taken in a risk-based approach;
   a) Continuation of the relationship with the customer,
   b) Preservation of the customer relationship through a close examination of its transactions,
   c) Terminating the customer relationship by closing the accounts,

2.6.4. Reporting Suspicious Transactions to Public Authorities

Suspicious transactions shall be reported to MASAK via its website or other methods determined by MASAK in maximum 10 business days after the date it was detected.

2.6.5. Non-Disclosure and Confidentiality

The information about suspicious transactions shall not be disclosed to related parties and third persons except to the authorities that are legally deemed appropriate to be informed.

2.6.6. Administrative Sanctions against Violation of Obligations

Administrative fines are applied in the following cases;

- Not applying relevant procedures with regard to ID checks and verifications,
- The staff members who do not report or repeatedly neglect his/her reporting obligation with regard to the assets acquired illegally or used for illegal purposes or notice any fact, detail, have any doubt or face with anything that may lead him/her to suspicion
- Violation of the obligation to provide continuous information,
- Failing to fulfill the electronic notification obligation,
- Those who do not fulfill the deficiencies regarding measures such as risk management, monitoring and control, internal audit within the period given by MASAK

2.7 Asset Freezing Decisions

The Bank's objective is to ensure compliance with international sanctions, including economic, commercial, or financial measures stipulated by authorized bodies of the Republic of Türkiye—primarily those under Laws No. 6415 and 7262—as well as those established by local or higher regulators in other countries where the Bank operates, and additionally by the UN, OFAC, EU, HMT, CBB and other generally accepted organizations and institutions.

In this context:

a) Decisions on asset freezing and the removal of such decisions are implemented promptly after publication in the Official Gazette.
b) For customers subject to asset freezing decisions, the type of business relationship, customer/account number, and the amount/balance of rights and receivables are reported to MASAK within the legal period.
c) All credit and bank cards belonging to individuals whose assets have been frozen are blocked, and access to internet banking, mobile banking, and other non-face-to-face systems is restricted.
d) In cases of any increase in frozen assets, such increases are also subject to asset freezing provisions. Therefore, access to any revenues, including profit shares, dividends, and other income from frozen assets, is only possible with MASAK's permission.
e) In electronic fund transfers, the Bank monitors and controls asset freezing lists concerning its customers who are party to the transactions.
f) If in bank transfer/EFT/FAST amounts are received in an account belonging to a person subject to an asset freezing decision, such increases in the account are subject to asset freezing provisions and reported to MASAK.

For SWIFT transactions, monitoring and control activities include verifying whether the recipient or sender is on the asset freezing (MVD) lists.
If the SWIFT transaction recipient holds an account with a financial institution abroad and is found on the MVD lists, the Bank enforces asset freezing measures and informs MASAK. Subsequently, the transaction amount involved in the SWIFT transfer is allowed to be transferred to a bank account in Türkiye belonging to the person or institution subject to asset freezing, with MASAK's permission.
Similarly, if the SWIFT transaction sender holds an account abroad and is on the MVD lists, the Bank enforces asset freezing measures and informs MASAK. The transaction amount involved in the SWIFT transfer is then allowed to be transferred to a bank account in Türkiye belonging to the person or institution subject to asset freezing, with MASAK's permission.
In SWIFT transaction controls, measures are taken to track matches based on a specific similarity ratio rather than exact matches, to identify potential matches.

g) In cases of non-compliance with obligations, administrative or judicial fines, or imprisonment may be imposed under Article 15 of Law No. 6415.

Procedures related to asset freezing decisions are carried out in accordance with documents such as created procedures, implementation manuals, workflow diagrams, instructions, etc. All such documentation is kept on the intranet, accessible to Bank staff.

3. MONITORING AND CONTROL POLICY

3.1. Purpose

To protect the Bank from risks and constantly inspect and control the compliance of activities of the Bank with the law and the regulations/communiqués drafted regarding prevention of money laundering and funding terrorism, and with the Bank's policies and procedures.
Monitoring and controlling activities shall at least include the following activities;

a) Monitoring and controlling the customers and transactions in the high risk group,
b) Monitoring and controlling transactions conducted with risky countries,
c) Monitoring and controlling complex and unusual transactions,
d) The Bank's control, through sampling method, of whether the transactions exceeding the amount, which the Bank will determine according to the risk policy, are consistent with the customer profile,
e) Monitoring and controlling linked transactions which, when handled together, exceed the amount requiring customer identification
f) Control of customer related information and documents which are required to be kept in electronic environment or in written form and the information required to be placed in wire transfer messages, getting the absent information and documents completed and updating them,
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 based control of services that may become prone to misuse due to newly introduced products and technological developments.

3.2. Monitoring and Control

The following subjects and transactions must be checked based on minimum transaction amount or periods determined by the Legislation and Compliance Department periodically:

3.2.1. Risky Customers

1. In respect with information taken while creating customers among PEPs and providing services to them,
2. The transactions made by charity and welfare organizations (voluntary donations and welfare clubs), shall be monitored within risk-based approach and their source, purpose and relevance with the customer profile are determined. The shortcomings detected shall be reported to the related branches/units and their results are must be monitored.
3. About the banks with which we will have correspondent banking transaction;

a) Their field of activity, prestige and efficiency of their internal and external supervision,
b) Whether the banks has gone under any investigation, inquisition, prosecution or penalized on charges of money laundering and funding terrorism,
c) Procedures they apply about prevention of money laundering and funding terrorism,
d) Changes in their top managements,
e) Correspondent banks shall be monitored to detect whether any of them has any customers allowed to access their accounts directly or not. If any of them has such customers, the bank shall be monitored to find out whether it is fulfilling its obligations with regard to giving special attention to such customers or not. Any deficiencies found, must be reported to the related units and the results followed.

4. The transactions related to the customers in high risk sectors and business lines identified by the Legislation and Compliance Department, their documentation, purpose of transactions and relevance of the stated purpose to customer's main field of activity, the source of the transaction amount must be monitored and any missing information detected must be reported to related branch or unit for appropriate action.

3.2.2. Risky Transactions

a) The system approval shall be taken from branch operators for cash transactions within risk-based approach.
b) The system approval shall be taken from branch authorities for electronic fund transfers. The relevance of the transactions to customer profile, to its purpose, the information and documents about transfer orderer and beneficiary shall be controlled. The shortcomings detected shall be reported to relevant branches/units for taking necessary measures.
c) Regarding personal cheques drawn on banks abroad; The service of cashing foreign exchange cheques can be rendered only to persons or firms having solid commercial past and credibility, whose physical assets and business volume are in correlation with amounts of the cheques, and whose business ethics and commercial practices are known in detail. The relevance of transactions to the purpose of the ones declared by the customer earlier shall be controlled. The shortcomings detected shall be reported to relevant branches/units for taking necessary measures.
d) The credits with cash blockage guarantee may be allocated to the companies and people that we have detailed information about their trading operations and business ethics.
e) Branches are obliged to monitor the frequent users of safe deposit boxes to find out whether they are involved in any illegal activity or not.

3.2.3 Transactions Requiring Special Attention

Special attention shall be paid to complex and unusual large transactions and the ones which have no apparent reasonable legitimate and economic purpose, to take necessary measures in order to obtain adequate information on the purpose of the requested transaction, and to keep the information, documents and records obtained in this scope in order for submittal upon request of authorities.

3.2.4 Monitoring the Customer Profile and the Transactions

The Bank shall follow up permanently the transactions conducted by customers whether they are in compliance with the information regarding the customer's profession, commercial activities, business history, financial status, risk profile and sources of funds within the scope of permanent business relationships and keep up-to-date information, documents and records regarding the customer. Furthermore, the accuracy of information regarding the telephone and fax number and e-mail address of customers received for customer identification shall be verified, if necessary, within the scope of risk-based approach using these means by contacting with the relevant person. Necessary measures shall be taken in order to follow up the transactions conducted out of permanent business relationship in risk-based approach. The Bank establishes appropriate risk-management systems with this purpose.

3.2.5 Simplified Measures

1) The Ministry may allow obliged parties to take more simplified measures in terms of customer due diligence in the following situations;
   a) In transactions carried out between financial institutions on behalf of themselves,
   b) In transactions where the customer is a public administration, quasi-public professional organization and state-owned enterprises regulated by the Decree-Law on State Economic Enterprises, dated 8/6/1984 and numbered 233
   c) In establishing a business relationship within the scope of salary payment by accepting a batch of customers,
   d) In transactions related to pension schemes that provide retirement benefits to employees by way of deduction from their salaries and of pension agreements,
   e) In transactions where the customer or his partner with a majority share exceeding 50% is a company whose shares are quoted in Borsa İstanbul.

The Ministry is authorized to determine transaction types other than those mentioned above in situations where the measures to be implemented under this article and the risk-based approach assess the risks of money laundering and financing of terrorism as low.

2) The Bank may not apply simplified measures in cases where money laundering or terrorist financing risks might occur due to the transaction and shall take into account that the transaction is possibly a suspicious transaction.

3.2.6 Enhanced Measures

1) The Bank shall apply, in proportion to the identified risk, one or more or all of the following enhanced measures for transactions within the scope of transactions requiring special attention, technological risks and risky countries and for high-risk situations they identify in the framework of risk based approach.
   a) Obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner,
   b) Obtaining additional information on the intended nature of the business relationship,
   c) Obtaining information, to the extent possible, on the source of the asset subject to transaction and source of funds of the customer,
   d) Obtaining information on the reasons for the transaction,
   e) Obtaining approval of senior manager to commence or continue business relationship or carry out transaction,
   f) 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,
   g) Requiring that in the establishment of permanent relationship the first financial transaction is carried out through another financial institution subject to customer due diligence principles.

3.2.7. Risky Regions

a) The transactions from the regions described as risky by System which exceeds the lower limit determined by the Legislation and Compliance Department,
b) The transactions chosen by sampling method about the citizens, companies and financial institutions in the countries which appear in the FATF's list of non-cooperative countries for not applying FATF recommendations or applying them imperfectly,
c) The transactions that are chosen by sampling method about the persons settled in the anti-democratic countries and regions which are situated on illegal drug production-distribution routes and where the rate of crimes such as smuggling and terrorism is high and corruption and bribe is common,
d) The transactions about the people settled in offshore centers, free zones and international finance centers where strict confidential laws are applied on banking practices, shall be scrutinized; the documents declared, the purpose of the transaction, its connection with the customer's business line, the sources of the amount shall be created while creating a customer relationship with any of these people and the shortcomings detected shall be reported to the concerned branch/unit for appropriate actions. Results of the actions taken must also be controlled.

3.2.8. Complicated and Unusual Transactions

The transactions which are of complicated or unusual nature shall be monitored in accordance with the procedures and periods determined by the Legislation and Compliance Department.
A report must be prepared about the shortcomings found in the course of the controls of these types of transactions. The report shall be given to the concerned branches/units for taking necessary actions. Results of the actions taken must also be controlled.

3.2.9. Connected Transactions

The following banking transactions which do not require permanent customer relationship shall be monitored in accordance with the procedures and periods set by the Legislation and Compliance Department:

1. Transfer/EFT.
2. Cheques/bills/notes collection.
3. Bill payments.
4. Foreign exchange transactions.
5. Other payments.

If a customer has the transactions mentioned above and the total amount of these transactions equals or exceeds the amount specified in the Regulation on Measures to Prevent Money Laundering and Financing of Terrorism (or its equivalent in foreign currencies), ID checks and verification must be applied. Whether the checking and verification in this regard is fulfilled or not must be controlled. The discrepancies and shortfalls detected shall be sent to the relevant branches/units for appropriate action and the results shall be monitored.

3.2.10. Virtual Transactions/Transactions Done by Using New Products and Recent Technological Developments which are Prone to Abuse (Internet, Mobile, Call Center, POS and ATM transactions)

The transactions of those customers which frequently prefer alternative distribution channels instead of using the branch network shall be monitored in accordance with the procedures and periods established by the Legislation and Compliance Department.
A report must be prepared about the missing data and documents found in the course of the controls of these types of transactions. The report shall be given to the concerned branches/units for taking necessary actions. Results of the actions taken must also be controlled.

4. TRAINING POLICY

4.1. Purpose:

To ensure compliance with the obligations resulted from laws, regulations and communiqués regarding prevention of money laundering and funding terrorism and to create a corporate culture by enhancing the sense of responsibility among staff about the Bank's policy and procedures with a risk-based approach, and, to keep updated.

4.2. In-House Training Programs

Under the supervision and coordination of the Compliance Officer, trainings (in accordance with their duties and responsibilities) should be provided regularly to all Bank staff, especially those who are in a one-on-one relationship with the customer, about the prevention of money laundering and terrorist financing.
Training programs shall be approved by the Board of Directors. The principles and methods of choosing the content of training programs and the participants will be determined by the Legislation and Compliance Department.
Trainings shall be given within the framework of the Bank's Training Policy, in the form of formal education, in-branch training, seminars and conferences and online training. In addition to these, staff must be frequently informed about the changes in national and international law, regulations and laundering typologies through the intranet system.
Staff members are trained about the following subjects:

a) Laundering proceeds of crime end terrorist financing,
b) The stages, methods of laundering proceeds of crime and case studies on this subject,

c) Legislation regarding prevention of laundering proceeds of crime and terrorist financing,
d) Risk areas,
e) Institutional policy and procedures,
f) Principles relating to customer identification,
g) Principles relating to suspicious transaction reporting,
h) Obligation of retaining and submitting,
i) Obligation of providing information and documents,
j) Sanctions to be implemented in violation of obligations,
k) The international sanctions and regulations on combating laundering and terrorist financing,
l) Information sharing within Financial Group,
m) Asset Freezing, Prevention of Financing the Proliferation of Weapons of Mass Destruction, and Sanctions

The staff undergone the training programs shall take an exam following the program to assess whether they have reached the required knowledge level or not.
Training activities are subject to review with the participation of the relevant departments according to the results of measurement and evaluation and are repeated at regular intervals as needed.
Trainings on prevention of money laundering and terrorist financing should be provided to the new joined staff within three months from the date of employment by the department responsible from the training activities. Penalties for the staff who have not completed the training within this period are determined and followed by the relevant unit.
Moreover, the training materials prepared and updated by the Compliance Officer will be available on the intranet system and easily accessible by all staff of the Bank. All developments, regulations, communications and lists of objectionable persons and organizations about prevention of laundering, funding terrorism and customer identification will also posted on the intranet and computer automation system where they can easily be accessed by all staff.
The statistical results (number of the staff that have attended the training and the total training hours etc.) of training programs shall be given to the Compliance Officer by related department. The results, then, shall be submitted to MASAK by the Compliance Officer before 15th of March, in the following year with a cover letter.
a) Training programs shall be submitted to Board of Directors for approval in its last meeting of each year.
b) In case of training services, which will be procured externally, a request shall be made to related department after the instructor's and supplying firm's efficiency is assessed by the Legislation and Compliance Department.

4.3. Training Programs Organized by Financial Crimes Investigation Board (MASAK)
The Legislation and Compliance Department will organize the training programs that MASAK will offer to the staff members of the Bank. The Bank's officer that will give in-house training for staff members must have the "instructor" certificate provided by MASAK.

5. AUDIT POLICY
5.1. Internal Audit and Reporting Activities
Inspectors and auditors of Inspection and Internal Control units, conduct inspections and examinations with a risk-based approach, throughout the year to ensure the Board of Directors that the Compliance Policy is efficient and adequate, covering the following areas;
1. Bank's policy and procedures,
2. Risk management activities,
3. Monitoring and controlling activities,
4. Training activities;
   a) Whether they are adequate or not
   b) Their efficiency
   c) Whether the transactions are conducted in accordance with laws, regulations and communiqués.

In this context, the control points of the Compliance Policy's monitoring/controlling and risk management parts are audited. Deficiencies, errors and abuses revealed as a result of the internal audit, and opinions

and suggestions to prevent their re-emergence are reported to the Board of Directors. While determining the scope of the audit, the deficiencies identified in the monitoring and control studies and the risky customers, services and transactions are included in the scope of the audit.
While determining the departments and transactions to be audited, the size and transaction volume of the Bank are taken into consideration. In this context, it is ensured that units and transactions in quantity and quality that can represent all transactions carried out at the Bank are audited.
The statistical lists prepared jointly by Inspection Committee and Internal Control Unit with regard to inspection and monitoring activities (showing the number of the branches audited, and the number of transactions monitored with the aim of identity verification and detection of suspicious transactions) shall be submitted to the Compliance Officer by 15th of March in the following year.
Then, the lists shall be forwarded to MASAK with a signed cover letter by the Compliance Officer before the end of March.
In addition, reports on the activities of the Legislation and Compliance Department are regularly submitted to the Audit Committee, the Board of Directors and the ABG Compliance Officer.

6. INFORMATION SHARING POLICY WITHIN FINANCIAL GROUP

1. In order to ensure that proper measures within the scope of the compliance program are taken at the Group level, the affiliates of the Group can share information about the accounts, transactions and KYC information of the customer. Confidentiality provisions written in special laws do not apply to in-group information sharing.
2. Those working in organizations affiliated with the Group cannot disclose the information they have learned within the scope of the first paragraph and cannot use it for the benefit of themselves or third parties. In this context, sanctions in the relevant laws are applied to those who disclose information that should be kept confidential.
3. Along with the Financial Group Compliance Officer, the Board of Directors of the Main Financial Institution is also responsible for taking the necessary measures to securely share information within the group. This responsibility also applies to the Compliance Officers of the Financial Institutions affiliated to the Group and the Boards of Directors of these Institutions.
4. Financial institutions affiliated with the group cannot share information regarding suspicious transaction reports.

7. OTHER POINTS

7.1. Safe Keeping and Submitting of Records

The following records shall be kept for at least 8 years as stated within the scope of the Law no. 5549 and regulations regarding the Law:

a) IDs and documents for recognition of customers and transaction profiles (from the closing dates of accounts),
b) The documents and records related to transactions (from the last dates of the transactions)
c) Control and monitoring reports, the lists and documents regarding investigation of the transactions (from their editing date),
d) Reports of suspicious transactions forwarded to Public Authorities and the documents used to prepare such reports (from their editing date),
e) Training documents and attendance lists (from their editing date),
f) Other documents containing legal reports, correspondence and information (from their editing date)

7.2. Obligation of Providing Information and Documents

In order to fulfill the obligations arising from the Law, when requested by Legislation and Compliance Department or auditors the Bank staff shall fully and accurately provide 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.

8. REVIEW OF THE POLICY

This Policy will be reviewed annually by considering;

- National or international legislative changes,
- In-bank application changes,
- Changes in sector practices,
- Evaluations and recommendations by internal and external auditors
- Any recommendation by ABG

unless it is required to be revised in shorter periods.

In case this Policy is revised, the notification of the relevant changes to the staff can be made via electronic media such as intranet, extranet, internal memorandums, announcement or e-mail by receiving read receipts.

9. EFFECTIVE DATE

This Policy shall take immediate effect after the approval of the Bank's Board of Directors.